Policy Framework for Interpreting Risk in eCommerce Security

A Joint Research Project by :

Andersen Consulting

and

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

Printed on: 10/24/02 at 3:05 PM

Table of Contents

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

1 Introduction

As organizations rush to build and support eCommerce applications there is an increasing realization that information and financial assets are becoming more vulnerable to attack. Media hyped reports of the "BubbleBoy" virus and frequent network failure of eCommerce sites like e*Trade may serve to alarm the public, but the threats are real and the potential risks catastrophic. One industry survey discovered that "organizations engaged in Web commerce, electronic supply chains, and enterprise resource planning experience three times the incidents of information loss and theft of trade secrets than everybody else." [9]

Over 74% of senior executives responding to another recent industry survey believe their information security risks have increased over the last two years [10]. Other findings revealed that 82% of respondents appreciate the importance of information security and 75% indicate that their eCommerce efforts would expand if the risks inherent in the medium were reduced.

The financial risks are alarming [19]:

In 1999 $7.6 billion was lost in business productivity by Melissa, the Worm and other viruses

- International bank allows $12 million in unauthorized wire transfers due to insufficient EFT security
- Six million online consumers have been victims of credit card-related fraud or unauthorized use on the Web.
- The rate at which computer crackers are breaching corporate networks has nearly doubled in the last year, according to the 745 companies polled

Everyone knows that security is vital to eCommerce success. What they often don't know is that security is more than erecting physical and electronic barriers. The strongest encryption and most robust firewall are practically worthless without a security policy that articulates how these tools are to be used.

This paper provides a framework for managing information security policy for eCommerce applications. A security policy concern risks. It is high-level and technology neutral. Its purpose is to set directions and procedures, and to define penalties and countermeasures for noncompliance.

The Policy Framework for Interpreting Risk in eCommerce Security (PFIRES – pronounced "fires") addresses the need to unify security policies in a manner consistent with organizational eCommerce objectives. PFIRES also facilitates coordination and communication between senior executives, technology managers, and staff. This

framework takes a *life cycle* approach to reflect the frenetic real world of eCommerce where the furious pace of technological change presents both numerous business opportunities and increased risks. Although it appears there is no fail-safe way to guarantee security, there are measures -- as described in PFIRES -- that can be taken to reduce and manage risk.

Most organizations today operate like Nile.com, a fictitious online company that we will use to illustrate the PFIRES life cycle. Nile.com is a two-year-old Internet company that has trailblazed the market for online sales of cosmetics and toiletries. With some predicting that this market will total $50 billion by 2002, the vice president of marketing has determined that online auctions is the next big thing and has spearheaded a strategic makeover. Just in time for the holidays, Nile.com has revamped its web site and business model to include e-auctions, and this new direction appears to be gaining momentum.

Like most corporations, Nile.com has a set of information security policies, which are broadly defined to include any and all activities that are specifically intended to protect organizational information and information systems from loss, damage or unauthorized access [41]. It also protects against non-malicious losses such as accidents and mistakes.

Nile.com has information security policies to manage exposure to risk including the threat of unauthorized access and damage to sensitive corporate data. Unauthorized access can come from many sources, including hackers, competitors, or terrorist organizations. Damage may be incurred by viruses and worms, natural disaster or disgruntled current and former employees.

Nile.com is on the right path in terms of its security policy. The company has assessed the potential impact of risks such as those highlighted above in financial terms and has allocated resources (personnel, time, technology) to create and maintain policies to prevent losses from the identified potential risks. For example, its password policy regulates the proper format and change frequency and its intrusion detection policy dictates how network breaches are handled.

However, Nile.com's policy implementation suffers from the same problems as many organizations. Its intrusion detection policy was set in response to a hacking attempt by a rival eBusiness, an event that illuminated a weakness in its information security infrastructure. Its privacy policy, which was adequate in the days of e-tail, is no longer aligned with corporate strategic objectives of e-auctioning. Furthermore, its extranet policy has not been updated to reflect changes in the business environment, including increased competition and technological advances. Finally, its password policy is ineffective due to a lack of consistent enforcement and education among users.

The best approach to managing Nile.com's and any organization's eCommerce information security risk is the application of a formal and comprehensive policy framework like PFIRES.

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

1.1 Audience

This research effort is targeted toward two audiences. The first is the executive level -- either the Chief Information Officer (CIO) or Information Technology (IT) department -- the individual or department charged with steering information technology strategy. PFIRES will help guide top executives through the difficult stages that must be addressed during the life cycle of a security policy.

The second target audience is comprised of information and security professionals – the real people who carry out executive directives. For this group PFIRES is a practical guide through the policy implementation.

1.2 Scope and Assumptions

The PFIRES model offers an excellent starting point for understanding security policy's impact on an organization, and is intended to guide organizations in developing, implementing, and maintaining security policy. The scope and limitations of the research presented in this document are outlined below.

1.2.1 Scope

Because of the large and growing number of eCommerce applications and related security issues, the scope of this paper is necessarily limited. Specific products, vendors, and implementation and maintenance issues are intentionally omitted. Industry-specific concerns are highlighted but not explored. Similarly, international and intellectual property rights, although significant, are not explored in any detail. Additionally, specific organizational behavior issues relating to information security in eCommerce, such as policy non-compliance, are not covered in depth. For these out-of-scope issues, references to other resources are provided where possible.

1.2.2 Assumptions

While creating this policy framework these assumptions obtained. We assume that either securities policies are currently in place or are under development. We assume that effective management of security policy is an important priority for top executives. We also assume that a security team is already in place.

1.3 Purpose

Our purpose is to provide information security professionals and top management a framework through which useable security strategy and policy can be created and maintained in line with the standard information technology life cycle.

1.4 Paper Organization

The remainder of this paper is organized as follows. Section 2, Background, presents the current state of affairs in information security policy for eCommerce, some of the key participants in this research effort and the context for the framework. In Section 3, the framework itself is introduced and each step of the life cycle is described in depth. The paper concludes in Section 4 with remarks about future concerns. The appendix contains a cost/benefit model to assist presenting the justification of expenditures on security, a glossary of terms, and a reference list.

When appropriate we have used an imaginary company, Nile.com, to illustrate a typical organization's concerns, problems, and successes with following PFIRES. The inclusion of a fictitious organization is not meant to trivialize the issues of policy development; our intent is to demonstrate the application of PFIRES in a business situation occurring daily – a company embarking on strategic eCommerce changes.

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

2 Background

The basic requirements for eCommerce security include information confidentiality, authentication, authorization, data integrity, non-repudiation [2] and availability. Given the dynamic environment of eCommerce, effectively meeting these requirements is not straightforward. The challenge is to come up with the most technically and economically feasible plan for protecting eCommerce activities, knowing that today's most secure technology will be vulnerable tomorrow.

As is the case for most systems problems, the best approach is a structured one, including analyzing risk and delegating resources to protect the most valued assets of the organization. Typically, policies are put into place to manage risk. Literature on how to develop specific Internet and information security policies may be found in [24], [35] and [40]. Another framework for developing eCommerce policies uses a matrix of organizational relationships and technology [27]. The problem with current approaches is that none address the problem of keeping up with the increasing rate of change in eCommerce technology and applications nor do they consider how to keep such policies consistent and aligned with organizational objectives.

To develop a tool that would aid in the formulation and management of eCommerce information security policies, other tools in similarly rapidly changing business arenas were examined. PFIRES was developed borrowing from both the new product development life cycle [16], [38], and the systems development life cycle [17].

2.1 Defining Security Policy

Security policies are generally high-level, technology neutral, and concern risks. Security policies set directions and procedures and define penalties and countermeasures if the policy is transgressed. Nile.com's access control policy, for example, reads "all user identities accessing internal information resources from the Internet must be authenticated using a two-factor method". Security policies must not be confused with implementation-specific information, which would be part of the security standards, procedures and guidelines, none of which falls within the scope of this paper.

Security policies are created by empowered representatives from groups responsible for:

- Human resources
- Legal and regulatory matters
- Information systems
- Public relations

- Security
- Lines of business

Some of the most important security policies include:

- User identification and password policy
- Remote access policy
- Extranet policy
- Internet security policy
- Access to data policy
- Administration policy
- Incident response policy
- Awareness procedure policy
- User behavior policy
- Security monitoring and audit policy
- Privacy policy

Security policies must be balanced and provide tradeoffs between:

- Level of security
- User convenience
- Cost

Without an equitable balance between these elements, it is not realistic to expect that the security policies will be followed. This may mean they should be modified. At Nile.com, for example, one of the technical managers is especially enamored of biometrics, and would like to implement iris scan technology to restrict access to eCommerce servers on site. Today, high cost and user inconvenience far outweigh the benefits so smart cards are used instead; however, as costs decrease and usability improves, her dream of biometric authentication may become a policy reality.

2.2 International Issues

One significant area of concern for eCommerce is the international nature of the Internet. Jurisdictional issues, intellectual property rights, laws regarding particular technologies (for example, encryption), local custom and local decency standards, and various political and terrorist

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

agendas, to name a few, all are cause for concern. But the boundaries of this paper do not allow an in-depth discussion of these issues. For additional information we recommend [22], [4], and [25].

2.3 Industry Issues

There are a number of industry-specific challenges when it comes to security. For example, an entirely online company like Nile.com may face different threats and risks than those faced by financial services or manufacturing companies. Instead of focusing these differences, we examine application-specific issues. For example, on-line transaction security for credit card processing is critical for several different industry areas including e-tailers like Nile.com, airlines and other service providers. Information about various challenges to different industries, types of organizations and applications can be found in [26] and [32].

2.4 Project Participants

The development of this framework was completed under the direction of the Center for Education and Research in Information, Assurance and Security (CERIAS) at Purdue University. Additionally, Andersen Consulting's Information Security practice, as well as faculty and students affiliated with CERIAS, aided the development effort. This combination of research and practical experience contributes to the comprehensive nature of PFIRESS.

2.4.1 Project Team

The following people were part of the project team:

Name	Organization
Shubo Bandyopadhyay	CERIAS
John C. Clark	Andersen Consulting
Bruce P. Coffing	Andersen Consulting
Daniel J. Deganutti	Andersen Consulting
Sharon K. Dietz	Andersen Consulting
Kevin Du	CERIAS
Scott Dyer	Purdue University
Stephanie Miller	CERIAS
Dr. Jackie Rees	CERIAS
Dr. Eugene Spafford	CERIAS
Mikko Rieppula	Andersen Consulting

2.4.2 Acknowledgements

The project team would like to thank the following individuals who

assisted, reviewed and/or provided guidance during the completion of this project.

Name	Organization
Greg Kapp	Purdue University
Andra Short	CERIAS
Caron S. Ellis	Andersen Consulting

2.4.3 Contacts

For further information regarding this project, please contact:

Name	Organization	E-mail
John C. Clark	Andersen Consulting	john.c.clark@ac.com
Andra Short	CERIAS	acs@cerias.purdue.edu

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

3 Policy Framework for Interpreting Risk in eCommerce Security

The PFIRES life cycle consists of four major phases: *Assess*, *Plan*, *Deliver*, and *Operate*. Each is sharply defined with specific exit criteria that should be met before transitioning to the next phase.

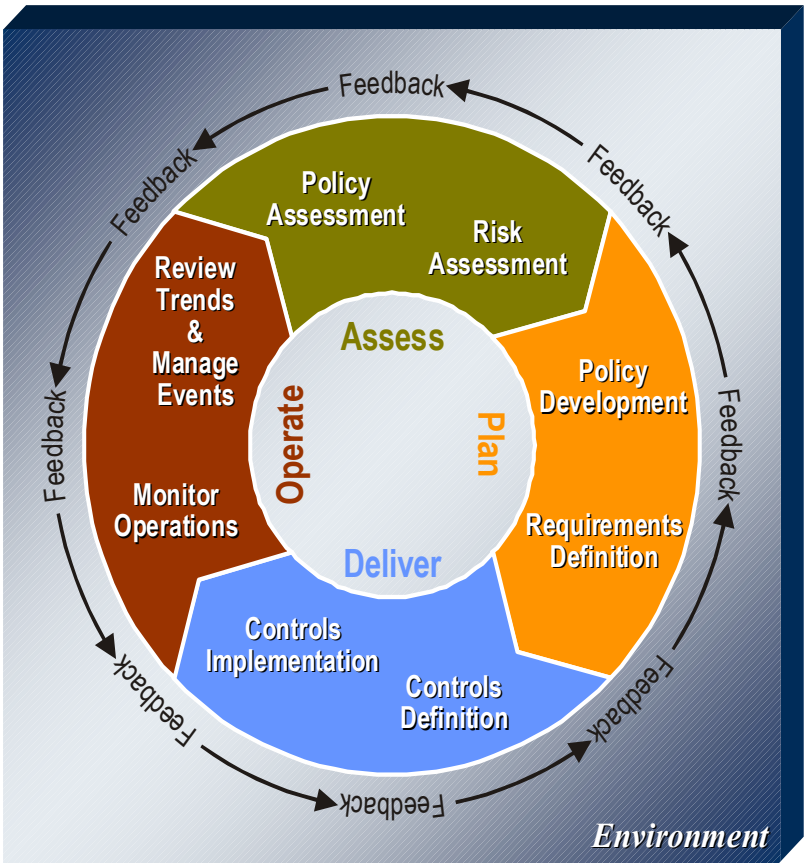

Figure 1: PFIRES Life Cycle Model

Each phase is further broken down into steps detailing the activities that occur within each phase. These steps are explored with particular attention paid to people, processes and technology issues.

It is important to remember that policy development is an iterative process. Therefore, the model includes feedback loops at every step. Feedback is also necessary to ensure that the requirements of the previous step, no matter where you are in the cycle, are being satisfied.

PFIRES was developed specifically for eCommerce security policy. As the CIO and technical staff of Nile.com well know, in the current eEnvironment, change is relentless and fast. Only yesterday the company sold soap and hairspray over the Internet; today it is auctioning everything from consumer electronics to vacations. By following PFIRES, Nile.com's security team is able to develop a security policy flexible enough to adapt to changing risks and requirements.

Copyright 1999, Andersen Consulting & CERIAS

3.1 *Assess Phase*

The *Assess* phase can be initiated by two distinct events: either a decision to execute the model from scratch or a response to a proposed change output from the *Review Trends and Manage Events* step. In either case, the goal is to assess the proposed change against the existing policy and organizational environment.

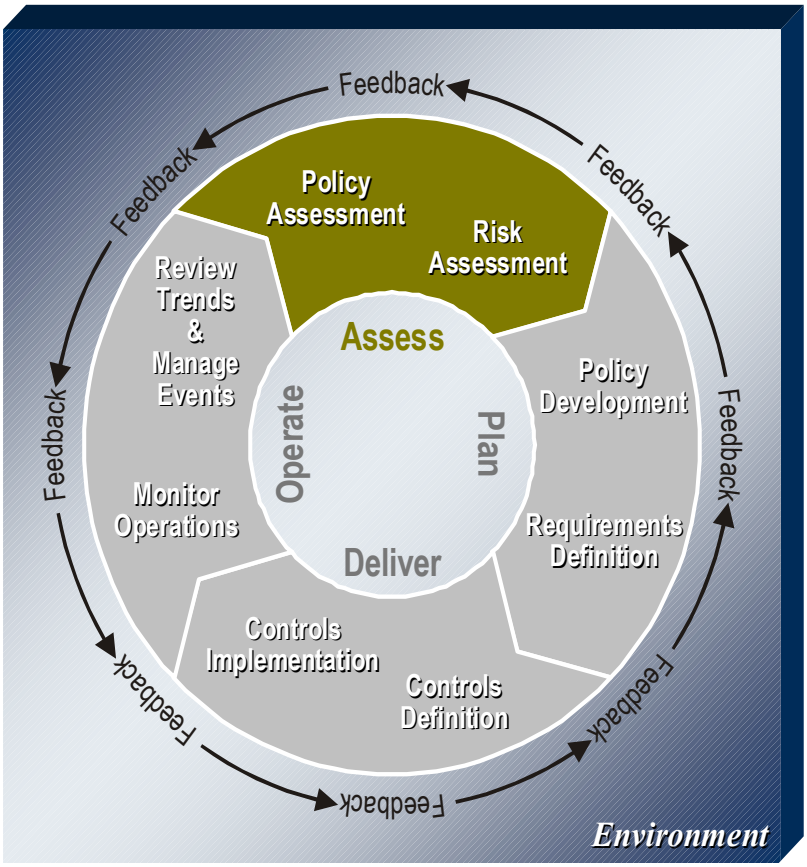

Figure 2: Assess Phase

The outputs of the *Assess* phase are:

- A completed Policy Assessment
- A completed Organizational "As-is" Assessment
- A completed Risk Assessment
- A decision on whether to implement the proposed change
- A communications strategy and plan

The *Assess* phase has three possible results:

- The proposed change is accepted. The *Plan* phase is initiated with

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

the completed Policy, Risk and Organizational "As-is" Assessments as input.

- The proposed change is not accepted but the Policy Assessment determines that policy should be updated. The *Plan* phase is initiated with the Policy Assessment as input.

- If the proposed change is not accepted and the Policy Assessment determines that policy does not need updating. The model resumes in the *Operate* phase.

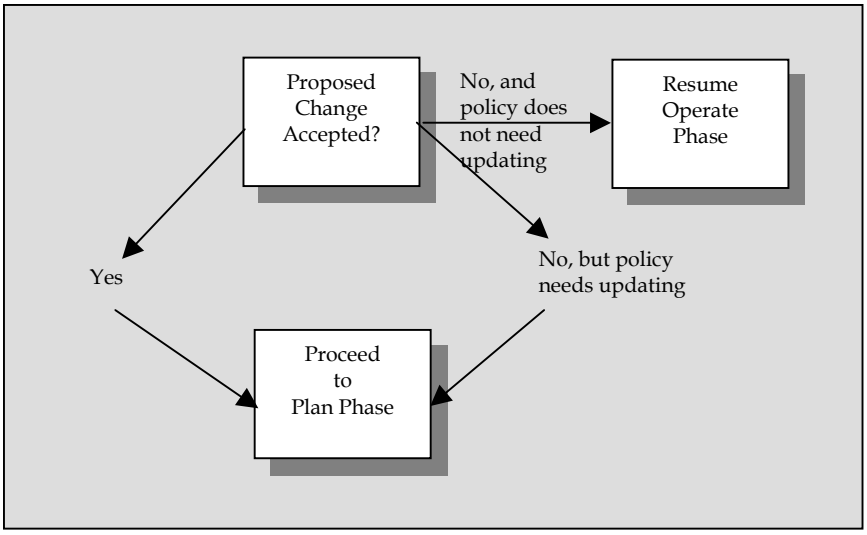

Figure a) Proposed Change Flowchart

Since this is Nile.com's first time executing the PFIRES model, the *Assess* phase is the logical starting point. However, before beginning the process of implementing security policy, the company needs to review existing policy and complete a full risk assessment. These are conducted during the two steps included in the *Assess* phase, *Policy Assessment* and *Risk Assessment*, which are examined in greater detail below.

3.1.1 Policy Assessment Step

Whether PFIRES is initiated due to initial policy creation or a change to existing policy, *Policy Assessment* is conducted to review existing policies, standards, guidelines and procedures.

Outputs of this step include:

- A determination of whether the proposed change is strategic or tactical in nature (i.e., the scope of the proposed change)
- An analysis of how the proposed change affects current policy
- An Organizational "As-is" Assessment
- A communications strategy and plan

The determination of whether the proposed change is strategic or tactical will affect how steps later in the life cycle will be explored; however, if this is the organization's first time executing the model, the effort is by definition strategic in nature. For example, the Nile.com is going through both strategic – entering the new marketspace of online auctions and tactical -- beefing up confidentiality through PKI (public key infrastructure) . But since this the company's first time using PFIRES, all considerations will be strategic.

3.1.1.1 Initial Policy Assessment

An organization that does not have an existing security policy always begins at this point. This may be a new organization like a start-up, a company with no security policy in place, or one that is replacing existing policy. Existing organizational strategy and policy should be referenced to gain context, and to ensure that policy is created in compliance with existing business strategies and policies.

3.1.1.2 Ensuing Policy Assessment(s)

Organizations like Nile.com that are revamping existing policies will engage in Ensuing Policy Assessments rather than initial ones. It only makes sense for Nile.com to reference existing business strategy and policy to gain context for the creation of new or modification of existing security policy. Along with a Risk Assessment, this process assists the company in assessing the proposed change, providing Nile.com's CIO sufficient data to decide whether to accept the proposed change.

3.1.1.3 Policy Assessment Methodology

Four sub-steps are contained within the *Policy Assessment* step: Analyze Policy Environment, Identify Policy Gaps and Contradictions, Summarize Policy Assessment Results, and Develop Policy Recommendations. Executed in sequence, these sub-steps result in a decision on whether to accept the proposed changes and an assessment

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

of how the proposed change affects existing policy.

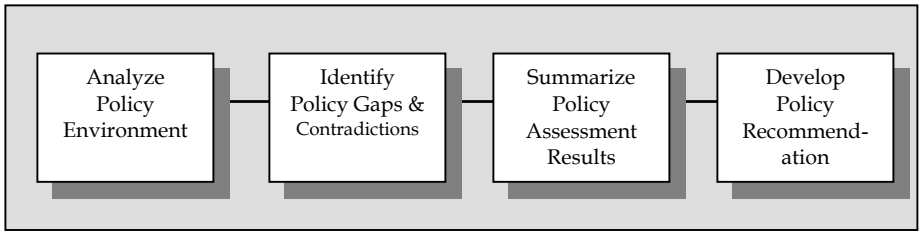

Figure b) Policy Assessment Sub-steps

3.1.1.3.1 Analyze Policy Environment Sub-step

If this is an organization's first time through the life cycle, this sub-step will be extensive, involving looking throughout the organization for existing policies, standards, guidelines and procedures, written and unwritten. Unwritten material will need to be documented, agreed upon by users, and approved by the appropriate management stakeholders. For subsequent iterations through the model, policy environment will have already been documented.

Documenting existing, unwritten policy is a very time-consuming task. At Nile.com, for instance there us an unwritten policy that user IDs are <LastName.FirstName>. But in order to discover this and any other unwritten policies, interviews should be conducted to identify existing documented policy and to determine which users are good targets to interview to uncover unwritten policy. Once Nile.com the interviews are complete, all discovered policy should be gathered, documented, and stored in a location readily accessible to all Nile.com members for future reference. During subsequent passes through the model, this collection can then be reviewed in light of any proposed changes being analyzed.

This is also the point in the model where an Organizational "As is" Assessment should be performed. For further information on this assessment, please refer to Section 3.1.1.5 Human Performance Implications.

3.1.1.3.2 Identify Policy Gaps and Contradictions Sub-step

This sub-step identifies the policies that the proposed change violates or contradicts along with any gap in policy brought to light by the current policy assessment. This process identifies areas affected by the proposed change so that they can be addressed during later steps in PFIRES. Both new policies that will need to be created along with old policies that will need to be updated, should the proposed change be approved, are identified.

It is important to note that policy should also be reviewed when the proposed change *is not* approved since rejection may uncover the need to update policy as well. For example, before embarking on the PFIRES model, Nile.com had considered a proposal to allow streaming audio

traffic from the Internet through the firewall. However, with the increased traffic expected from the new eAuction offerings, streaming audio is both too bandwidth heavy and risky to be permitted. The proposed change, therefore, has been rejected. This policy gap reveals that the company's policy needs to be updated to reflect that this type of network traffic is not allowed.

3.1.1.3.3 Summarize Policy Assessment Results Sub-step

This sub-step documents the policy gaps and updates that need to be addressed both for approved and rejected changes, and produces an outcome document, Policy Assessment Results.

3.1.1.3.4 Develop Policy Recommendation Sub-step

The goal of this sub-step is to produce a recommendation to approve or reject the proposed change based on policy assessment.

To ensure that strategic business drivers for the proposed change are weighed fairly against the policy assessment results, it is important that security staff work closely with management to review Policy Assessment Results. Their resulting recommendation will also be documented in Policy Assessment Results. This recommendation will be taken into consideration with the results of the risk assessment to determine whether the proposed change will be approved.

For Nile.com, the proposed changes concerning confidentiality and authentication will probably receive a favorable policy recommendation since they are entirely in line with corporate strategy.

3.1.1.4 Policy Assessment Scope

On a continuum of change, we define the two end points as tactical and strategic. Tactical changes are those which involve short-term goal achievement and how to control and evaluate the process of achieving goals, whereas strategic changes are long-term, broad-based initiatives that involve positioning within the marketplace and typically involve members of senior management [30]. Most changes organizations face will fall somewhere in between these two end points.

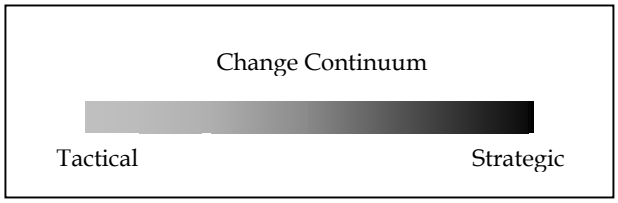

Figure c) Change Continuum

Once the policy assessment is complete, a decision needs to be made on where within the change continuum the proposed change falls. The position on the change continuum that the proposed change falls will

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

help determine the scope of the *Risk Assessment* step, therefore influencing the execution of the subsequent steps of the life cycle. Note that if this is the organization's first time through the model, the effort is always strategic in nature.

3.1.1.5 Human Performance Implications

When we speak of human performance, we are talking about a complex adaptive system, like an ecosystem or the system of a human body. Human performance involves the performance of business processes by employees, of course. But it also involves the abilities and motivation within people that give rise to performance; it involves the management actions that influence employee capability and motivation; it involves occurrences in the business environment of the company that give rise to organizational strategy. You cannot speak of any one part of the system of human performance without speaking of all the parts.

Nile.com management wisely recognizes that a successful change in security policy involves people who must understand and follow it. Therefore the company is implementing human performance activities designed to minimize the risks of the policy not being executed and to ensure that its new policies have the greatest probability of success.

As is well-known, commitment is a key factor to successfully implementing change [8], and demonstration of commitment through strong executive sponsorship is critical to embarking on any change initiative. At Nile.com, sponsors include the CEO and CIO who will authorize and enforce the new policy and any subsequent changes. They understand that clearly communicating their commitment to the security policy life cycle and promoting their security goals and expectations will go a long way to providing both guidance and support [8], [13], [33].

Communication at Nile.com, and any organization implementing security policy change, will need to occur between users, the security organization, and executives. A communications strategy provides the vision for communication and involvement activities and details how they support the overall human performance goals. Questions addressed through this strategy include "where do we want to be?" and "what do we want to achieve through communication?" Nile.com executives are answering these questions by reiterating the company's new mission: "to be the place to discover just about anything you want to buy online" and by focusing their communications on the need for shoppers to feel safe and enjoy the experience of buying at Nile.com.

Additionally, a communications plan will outline the tactics needed to achieve the communications strategy, including all planned communications, target audience, dates, and individuals responsible for the communication. At Nile.com this means that the CEO's weekly memo will include security messages, an IT manager will make follow-up phone calls to supervisors, and Human Resources will institute employee security surveys and award bonuses to the first ten employees who change their password at the newly-implemented every-six-week

password revision schedule.

The type and scope of human performance work in the *Assess* phase will depend on whether the change is strategic or tactical. If strategic, as in Nile.com's first go round through the life cycle model, it is important to create a business case for all human performance work in order for sponsors and key stakeholders to appreciate its value. The business results described will form the basis of an ongoing dialogue with the sponsor as well as communications to the organization.

If the proposed policy change is tactical, it is important that a Organizational "As-is" Assessment (described in Section 3.1.2.3) confirm that the organization is equipped to make and adhere to policy changes. This is only possible when employees are empowered to do so and a good communications plan is in place.

3.1.1.6 eCommerce Implications

The rapid rate of change in eCommerce -- even for those companies already involved in eBusiness, like Nile.com -- has far-reaching implications for security policy. These changes, particularly the sharing of organizational information sources with customers and other participants in the supply chain, can have an enormous impact. Each proposed change must be reviewed carefully and expeditiously against existing security strategy and policy to ensure that existing policies are not contradicted and gaps in existing security policy are identified.

For example, Nile.com's proposed change to PKI necessitates using a certification authority (CA). Policy can either determine that the company operate an internal CA, outsource, or affiliate with a trusted third-party. Each of these choices may contradict an existing policy; in fact, the company already has a policy against doing business with any company that does business with its arch-rival in Canada. This eliminates a number of CAs, and may require additional work in the Identify Policy Gaps and Contradictions sub-step.

3.1.1.7 Conclusion

At the conclusion of the *Assess* phase, the proposed change has been measured against existing strategies and policies and has been identified as strategic or tactical in nature. Now we know what portions of the security policy need to be amended or created to support the proposed change. In addition, a recommendation based on the Policy Assessment is formulated. This recommendation will be taken into account together with the outcome of the risk assessment to determine whether the organization will accept the proposed change.

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

3.1.2 Risk Assessment Step

Risk Assessment identifies the business assets an organization wants to protect, and identifies potential threats to those assets by asking these questions:

- What am I trying to protect?
- What do I need to protect against?
- How much am I willing to spend to have adequate protection?
- What is the cost versus the benefit for the business?

3.1.2.1 Scope

Scope is determined by the strategic or tactical nature of the proposed change. A risk assessment for a proposed tactical change will focus on the immediate effects or context of the proposed change. Nile.com's upgrading to the latest version of a web browser would be tactical. The company's risk assessment for this proposed change would focus on the web browser, associated applications or applets, and the internal applications depending on information from and/or displayed through the browser.

A risk assessment for a proposed strategic change will focus on the entire organization. Nile.com's repositioning itself as an online auction provider is certainly strategic. Therefore, its risk assessment needs to focus on all aspects of the organization from the implementation of technology to allow for this change, i.e., PKI, to the processes of how the information is handled, i.e., customer privacy, to how this change will affect the people within the organization.

3.1.2.2 Risk Assessment Methodology

Risk Assessment consists of four sub-steps: Conduct Security Assessment, Assess Business Risk, Develop Security Recommendations, and Summarize Risk Assessment Results. Executed in sequence, these sub-steps result in a decision of whether to accept the proposed changes to security policy based on risk.

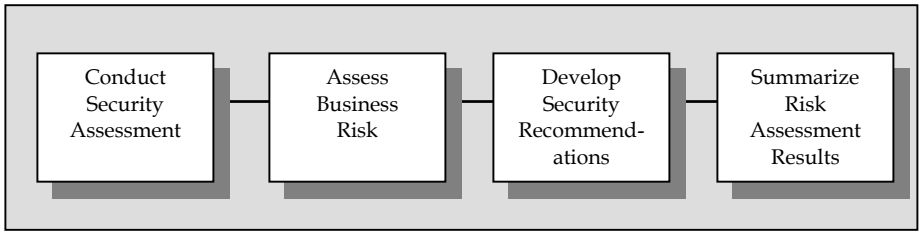

Figure d) Risk Assessment Sub-steps

Throughout the risk assessment process it can be helpful to document results in a spreadsheet-based matrix. For other examples see [28], [36], and [7].

Asset			Risk		
Asset Name	**Asset Type**	**Area to be Assessed (Technology, Platform, People)**	**Undesirable Events**	**Event History**	**Potential Damage**
Design documents	Customer Information	NT Server, network, Internet, firewall	A customer's competitor obtains access to proprietary design documents	Uncertain, no official record of it happening before, but rumors	Disclosure, modification or destruction of data, loss of customer confidence, lawsuit, fraud
Passwords	Technology	NT Server. User PC, Routers, Procedures, Awareness	Stolen password, misuse of authorized password	Employees have been fired for misusing access to commit fraud	Unauthorized access, masquerade, all data accessible by that account is exposed and subject to disclosure, modification and destruction
OS Software and configuration data	Technology	NT Server, Procedures, Training			
Help Desk	Application	UNIX Server, Training			
Engineering and scientific information	Administrative Information	NT Server, Users PC			
Product or service marketing plans	Administrative Information	Personnel	Marketing plan revealed to competitor	Several marketing staff, suspected but not proved to be involved in industrial espionage, jumped ship to competition six months ago	Disclosure could lead to not being first to market with a new offering

Figure 3: Risk Assessment Matrix

3.1.2.2.1 Conduct Security Assessment Sub-step

This sub-step identifies elements in the current or proposed environment

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

that may be subject to threats that could compromise information assets. Specific tasks include:

- Asset identification
- Threat assessment
- Vulnerability assessment

Asset Identification quantifies information system assets critical to the business including all forms of data and the people and technology that support information processes. Assets are then grouped to identify correspondence between the information assets and the technologies that support these assets; for example, Nile.com's customer list would be mapped to the server and database software that supports it.

Threat Assessment identifies threats to the confidentiality, integrity and availability of the identified assets. In general terms, a threat is a bad thing that can happen. For example, Nile.com's data center is located near a major geologic fault line, making earthquake a distinct threat. Threats can also be caused by direct or indirect actions which can originate from accidental or deliberate sources or events; Nile.com considers hackers and industrial espionage among these.

Vulnerability Assessment evaluates the target environment to identify weaknesses within the organization's assets that could be exploited and result in a compromise of assets. In general terms, a vulnerability is the weakness that allows a threat to happen. In Nile.com's case, locating the data center in a fault zone is the vulnerability.

A variety of methods can be used to analyze the environment including review of documentation, interviews with stakeholders, site surveys or walkthroughs, automated system and/or network assessments, and surveys of targeted groups. We suggest using a combination of these approaches to achieve maximum results.

3.1.2.2.2 Assess Business Risk Sub-step

This sub-step is a assessment of risk as it applies to business assets. Although we recommend a quantitative assessment, many organizations utilize qualitative measurements. In either case, each asset must be given a measure, which can be either intrinsic or related to the cost of restoration if the asset were to be lost or compromised.

The value of intangible assets, such as reputation and trust, that do not have any intrinsic or business value must be evaluated. One way to perform this evaluation is to list all assets evaluated so far, ranked in terms of value. Based on this list, the assets with intangible and subjective value will be inserted, according to best judgment, between two assets already evaluated.

The business impact loss or damage to business assets should be

evaluated and could include:

- Loss of reputation and client confidence
- Legal penalties against the company
- Cost of security failure recovery
- Cost of the unavailability of the system

This sub-step involves two tasks: Impact Analysis and Risk Valuation.

Analyze Impact identifies the effect on the business if the asset is harmed using two factors: potential damage and likelihood of occurrence. Damage is rated High, Medium, or Low Potential. For example, if loss of life is a possibility – as it would be in an earthquake -- the potential damage should be classified as High. Likelihood of occurrence is also rated High, Medium, or Low. For Nile.com, the likelihood of a hurricane directly hitting the Chicago sales office would be rated Low, but an earthquake at its data center would be High.

Risk Valuation determines a risk factor for each asset being analyzed. Risk, the potential damage or loss of an asset, is a combination of the value the owner places on the asset, the business impact the loss of the asset would have, and the likelihood that the weakness will be exploited to damage the asset. This risk factor can be assigned by a skilled security professional or calculated using the following formula:

Risk = Potential Damage x Likelihood of Occurrence

For each term in the equation, High = 3, Medium = 2, and Low = 1.

The risk factor is then assigned using the following chart:

Total Score	**Risk Factor**
1,2	Low
3	Low - Medium
4,5	Medium
6	Medium - High
7,8,9	High

For Nile.com:

Risk due to Earthquake = High Potential Damage x High Likelihood of Occurrence
Risk due to Earthquake = 3 × 3
Risk due to Earthquake = 9

The level of risk is an important input to calculating risk priority, which is then used to determine the priority of security recommendations to the business. Obviously, earthquake mitigation is a high priority for Nile.com.

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

3.1.2.2.3 Develop Security Recommendations Sub-step

The tasks involved with completing this sub-step are:

- Identify Security Options
- Determine Payroll and Non-payroll Cost
- Determine Priority of Options
- Verify Results
- Develop Cost/Benefit Matrix

Identify Security Options determines recommendations to mitigate each identified risk. This task produces the best conclusions when skilled security professionals work together to challenge each others recommendations. Two members of the security team at Nile.com, for instance, have different opinions on mitigating the earthquake risk. Both think Port Arthur, TX is the solution; however, one recommends a hot site, the other a mirror site.

Determine Payroll and Non-payroll Cost estimates a cost for each recommendation. Since licensing is done based on concurrent users' authentication, variables include the number of concurrent users the recommendation must support and number of management stations needed to support the solution. Non-payroll costs may include software, hardware (servers, workstations, network equipment), training equipment, and physical facilities.

To calculate the payroll cost of each solution, consider the total effort needed to plan, install test, train, and roll out the solution. Think about whether there are sufficient resources in-house to complete the project or if outside consultants will need to be hired.

Once the security options recommendations have been documented, they should be organized to Determine Priority of Options. The following factors can be used to calculate priority, and each should be rated either High, Medium or Low.

- Cost to Implement and Operate – What is the budget for the solution and does it fit within the department budget?
- Risk Level of the Vulnerability – How big is the hole the recommendation will fix?
- Effectiveness of the Solution – How well or completely will the solution work to resolve the vulnerability?
- Ease of Implementation – Are the skills needed to implement the solution available in-house or will outside consultants or contractors be needed? Will there be resistance to the solution from end users, operations, or management?

- Ease of Use – How much end-user and/or administrator training will this solution require? How many additional resources and/or steps will this solution add to the daily operation of the business? Will users be inconvenienced by the solution, and if so, what is needed to make it easier for them?

- Fit with Business Priorities – Is the solution in line with the information technology, business, and security visions of the company?

Priority can then be calculated by weighting each factor according to importance (w1, w2, …) using the following formula:

Priority = [Risk(w1) x Effectiveness(w2) x Ease of Implementation(w3) x Ease of Use(w4) x Fit with Priorities(w5) x Cost to Implement(w6)]

Verify Results confirms findings, assumptions, and recommendations with key management to ensure that the calculations based on these findings, assumptions and recommendations are accurate.

Finally, Develop Cost/Benefit Matrix documents the recommendations so management can view the options based on the value of the solution. Potential columns for the matrix include:

Option	Priority	Description	Bene-fits	Resources	Time to Implement	Non-payroll Cost	Implementation Plan
PKI	High	Widely-used encryption technique	Authentication	Staff needs training	Four weeks	$15,000	Choose vendor, Install, Train employees

Figure 4: Cost/Benefit Matrix

3.1.2.2.4 Summarize Assessment Final Results Sub-step

Here results of both the Policy and Risk Assessments are documented so management can decide whether to accept the proposed change. If accepted, the life cycle for this particular proposed change continues in the *Plan* phase. If rejected, but other policy changes are determined to be needed, the *Plan* phase follows as well. Otherwise, the life cycle resumes in the *Operate* phase.

3.1.2.3 Human Performance Implications

Policy updates or alterations will inevitably change something about the way someone is working, and such changes, no matter how small, require attention. The impact of the change must be assessed to make sure it can be successfully implemented. An understanding of the current environment is therefore vital. While some of the security team assesses the risk involved with the proposed change, others should

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

examine the existing organization structure, performance, and culture to determine the unique requirements of the proposed change. These questions should be asked to assess an organization's ability to successfully support a new security policy:

- Who is impacted?
- Does the organization structure reflect the importance of security?
- Is the culture conscious of the importance of security?
- Who are the key sponsors and advocates?
- How does the culture suggest components of a new policy and or highlight key implementation issues?
- What aspects of the culture suggest potential security risks that the new policy and implementation plan should address?
- What do you expect to happen when policy is implemented – what is the end result?

If these are not addressed the inability or unwillingness of the organization to change represents another potential threat to security.

3.1.2.4 eCommerce Implications

The process of moving business-to-consumer functions to an eCommerce model typically involves replacing the human intermediary with software. Historically, the human intermediary served several roles including information asset protection. Today the question the organization must ask is whether software can be skeptical enough to protect valuable information assets. Nile.com was founded as an eCommerce company, so it has already successfully faced many eCommerce risks. But the transition to online auctions means not only business-to-consumer risks but consumer-to-consumer risks as well. Therefore the company must ask whether software can be skeptical enough to protect the information asset of personal identification

3.1.2.5 Conclusion

If this is the organization's first time through the model, since there is no proposed change under consideration this step will address the risks inherent to the business. If there is a proposed change under consideration, it has been measured against the existing technical and organizational environment. The risk assessment has outlined what risks would be incurred by the implementation of the proposed change and steps to mitigate those risks. In addition, a recommendation based on the risk assessment has been formulated.

3.2 *Plan Phase*

As the second phase of PFIRES, *Plan* prepares for the implementation of the proposed change including creating or updating policy and defining the requirements for the proposed change.

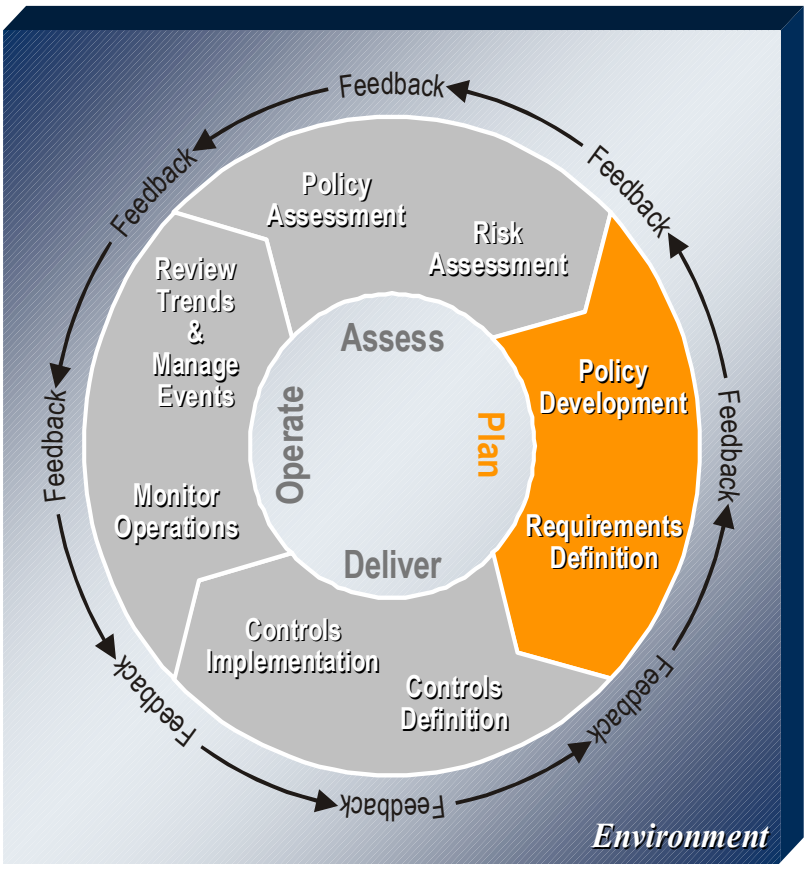

Figure 5: Assess Phase

The outputs of the *Plan* phase are:

- Created/updated security strategy
- Created/updated security policy
- Requirements for the change to be implemented
- Continued execution of the Communications plan

3.2.1 Policy Development Step

It is vital to develop security strategy and policy that is in line with existing business strategy and policy. Activities during *Policy Development* assure this.

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

3.2.1.1 Scope

Scope will depend on whether this is the first or a repeat time through the PFIRES model. If this is the first– Nile.com's situation -- a security strategy will need to be created or updated. If this is a repeat, security strategy will not need to be updated, so policy changes and/or updates will be limited to those related to the change being implemented. Bear in mind, however, that a security strategy, no matter how brilliant, should not be thought of as permanent. The nature of the Internet is constantly evolving; risks and threats to companies that rely on it are constantly evolving as well.

It is important to note that even if the proposed change was rejected, Policy Assessment might have determined that changes needed to be made based on that rejection. If that is the case *Policy Development* should be executed as well.

3.2.1.2 Policy Development Methodology

Policy Development contains two sub-steps: Create/Update Security Strategy and Create/Update Security Policy.

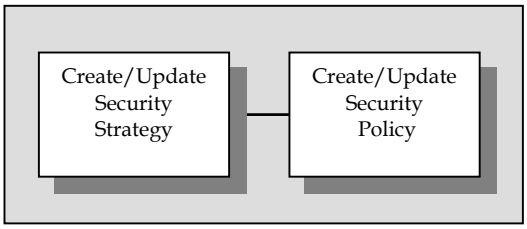

Figure e) Policy Development Sub-steps

3.2.1.2.1 Create/Update Security Strategy Sub-step

Security strategy is an overview of future business direction along with the security controls needed to support these business functions. A security strategy session should be held consisting of the following tasks:

- Identify future business initiatives
- Identify risks to each initiative
- Identify security options
- Prioritize security initiatives
- Document security strategy

This session should include key management personnel not only for their thought leadership but to gain their buy-in. Someone with security expertise and experience with facilitating high-level executives should facilitate. Discussions should cover the following topics:

- Future business initiatives with their associated security risks and concerns
- Prioritization of business applications and processes
- Prioritization of security initiatives
- Current security concerns of the business

Executive input is also vital to guarantee that security strategy is aligned with rest of the organization's business strategies. It will also ensure that security is considered when new business capabilities and acquisitions are planned, new alliances made, and new markets entered.

All strategies must work together. For example, Nile.com business, sales and marketing strategies state that customers should be allowed to check inventory in real-time over the Internet; therefore, the company's security strategy must reflect and enable this. If, however, IT determines that security concerns render this function too risky, business, sales, and marketing strategies must then be updated.

3.2.1.2.2 Create/Update Security Policy Sub-step

Specific tasks of this sub-step include:

- Identify Areas for Security Policy
- Draft Security Policy
- Review Security Policy
- Publish Security Policy

Additional information may be found in [28] and [40].

Identify Areas for Security Policy looks at Policy, Risk, and Organizational "As-is" Assessments to gather inputs in preparation for drafting security policy.

Draft Security Policy creates the initial version of the security policy or security policy update. Someone closely associated with the change – at Nile.com it's the director of network operations -- should be appointed the author. The security team should provide guidance to this person on the context and the content of the policy. The policy draft should include, at a minimum, the following sections or attributes:

- Title -- Provided by the security organization following a standard format.
- Version -- Version number of the document so it can be version controlled.
- Purpose

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

- Scope and Audience -- The intended audience and the environments to which it applies.
- Overview – A briefly explanation of relevant security issues including specific threats and vulnerabilities to consider.
- Roles and Responsibilities -- Define who is responsible for what actions.
- Content -- Identify and explain all relevant information.
- Reporting -- Information for reporting all security violations and security incidents.
- Related Documents
- Author and History – A record of the original author, authors of revisions, and a synopsis of each revision change.

Review Security Policy ensures quality, usability and acceptance of the policy. A small review team with user, management, and executive representation should review it. Their comments should be directed back to the author who will then make any updates deemed necessary. Then the final draft is forwarded to the security organization.

Finally, the Publish Security Policy task authorizes and communicates the policy. First, the security organization forwards the final draft to the executive responsible for approving the policy. Once approved, the policy is then communicated to the entire organization.

3.2.1.3 Human Performance Implications

Whether or not the proposed change was accepted, if there is policy development work underway, a communications plan will be needed to support it. Communications that enable audience feedback should be initiated during the *Policy Development* step to prepare the organization for upcoming changes and to enable individuals to influence the formation of the new policy. Involvement is critical in moving users through the stages of commitment from preparation through acceptance and ultimately to the commitment stage.

Interactive communication can be established using email or a web site. Nile.com sent out surveys via email. In order encourage speedy responses, a Starbucks gift certificate was awarded to employees who responded within 24 hours.

Key stakeholders should have deep involvement in the process of creating the new policy and contributing implementation ideas. This will not only contribute to the richness and appropriateness of the policy, but will also go a long way to assuring that the changes will "take". The team that forms the new policy should be a microcosm of the organization -- those responsible for security policy and enforcement, those who will be subjected to the policy, those who are served by the

policy, those with the authority to approve the policy – should all be represented. Nile.com, and many other organizations, also involve those who will be directly involved in implementation such as training, communications, and Human Resources. These experts can help ensure that the policy is usable, and thus accepted, by everyone in the organization.

3.2.1.4 eCommerce Implications

The process of moving business-to-business functions to an eCommerce model typically involves linking an organization to its suppliers, manufacturers, distributors, and retailers. In doing so, technical architectures become increasingly complex. With this increased complexity comes a tendency for the policy that controls this environment to become more flexible and less specific -- possibly opening up the organization to additional risk. As Nile.com revamps its network architecture to accommodate online auctions, it is finding that this is just the case; it must endure traffic with many more database, inventory, and customer servers than before. Therefore its security strategy and policy is being created to maintain control over all areas identified by the Policy, Risk and Organizational "As-is" Assessments.

3.2.1.5 Conclusion

If this is the organization's first time through the model, this step creates a security strategy and the body of security policy for the organization. For subsequent passes through the model, this step can update strategy and/or policy.

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

3.2.2 Requirements Definition Step

Within *Requirements Definition* an organization analyzes its security policy in order to define the requirements of the new security architecture in light of the updated policy. This step answers the question, "What needs to be done to implement the change?"

3.2.2.1 Scope

Unlike the previous steps, the scope of the *Requirements Definition* step is not dependent on the strategic or tactical nature of the change or on whether this is the organization's first time using PFIRES.

3.2.2.2 Requirements Definition Methodology

Requirements Definition consists of three sub-steps: Translate Recommendations to Requirements, Develop Detailed Security Requirements, and Verify Requirements.

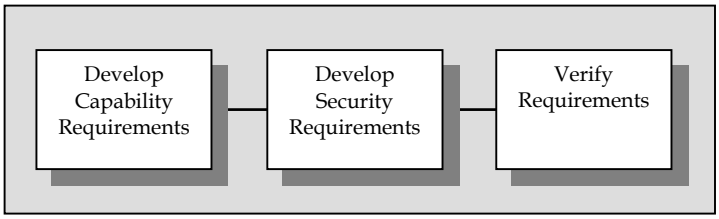

Figure f) Requirements Definition Sub-steps

3.2.2.2.1 Translate Recommendations to Requirements Sub-step

The high-priority recommendations developed in the Risk Assessment are used in this sub-step to create the security infrastructure necessary to support the change. Therefore, these recommendations must specify exactly the characteristics of that architecture. For example, since Nile.com's risk assessment recommended two-factor authentication to mitigate the threat of industrial espionage, this sub-step documents two-factor authentication as a requirement.

Of course, not all recommendations from the Risk Assessment will be translated into requirements, only those designated as necessary. Since the threat of hurricane in the Chicago sales office was deemed Low, Nile.com will not be incorporating any hurricane warning mechanisms into those requirements.

3.2.2.2.2 Develop Detailed Security Requirements Sub-step

Here the high-level requirements from the previous sub-step are built out into a sufficient level of detail so that control selection can begin. For example, Nile.com's "two-factor authentication" requirement is too generic to allow a thorough control selection. But detailed requirements

can include the portability of the two-factor device, specific systems it must integrate with, and even limitations on the range of options.

This sub-step carefully considers the overall technical environment so that the proposed change will tightly integrate and support the existing environment. Interoperability requirements such as systems and network support, and standards and API (application programming interfaces) support must be considered.

It is also critical to ensure that these requirements specify an adequate level of protection. Since they will be used in final control selection, inadequate detail may result in inadequate control selection. For example, Nile.com's security needs clearly call for encryption, but if the bit-length is not specified, 40-bit encryption may be selected for lack of detailed requirements.

Focused effort, and often a great deal of time, is required to complete successfully a detailed requirements definition. Additional best practices on requirements definition may be found in [12], [20] and [42].

3.2.2.2.3 Verify Requirements Sub-step

This sub-step validates the requirements defined in the previous two sub-steps against the inputs to the *Requirements Definition* step. All requirements should map back to a specific risk (as documented in the Risk Assessment) or to a specific point in the Security Policy. Mapping will ensure that all recommendations are being implemented and that extraneous requirements have not been introduced.

It is also important during this sub-step to evaluate the detailed requirements against industry best practices. Organizations should validate that they have considered industry-standard practices, whether or not they chose to adapt them. Additionally, market segments may need to meet requirements specified by their country or local government, or by some other authoritative body. For example, in the United States different segments of the telecommunications industry – of which Nile.com is a member by association -- are regulated by several local and federal bodies, along with numerous standards organizations.

3.2.2.3 Human Performance Implications

Thought must be given to not only how a policy change will improve security, but how it will impact individuals as they do their jobs. Some policy changes may result in job creation or redefinition. The Organizational "As-is" Assessment will be an important input into how to best adapt the new policy to the organization. Additionally, it will highlight some changes that the organization may need to make.

Representatives from training, communications, and human resources who participated in the *Policy Development* step will have to define the human performance requirements to support the proposed policy. For example, Nile.com's training experts will identify how to integrate the

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

policy into existing training for users, for example, how to create an easy-to-remember, hard-to-guess password. They may need to develop training for security professionals if new technology (for example, IPsec) is required to support the policy. The company's human resources experts may need to update or create job descriptions or review compensation levels if new, desirable skills (like Java programming) are required to implement new security technology. Communications experts will identify those being impacted by the proposed policy and how/when/what to communicate to them.

3.2.2.4 eCommerce Implications

The main eCommerce implication for the *Requirements Definition* step is speed. Indeed, Nile.com's transformation from e-tailer to e-auctioneer is taking a mere 90 days. Its well-defined requirements definition process stresses the importance of timeliness, but in order to achieve its goal safely as well as speedily, the company has placed great importance on the Verify Requirements sub-step. This sub-step provides the checks and balances needed catch any requirements that may have been missed in haste. Therefore the company identified knowledgeable reviewers from both the technology and business side for this sub-step.

3.2.2.5 Conclusion

Once the requirements have been verified, they will be used during the next step to verify that the planned controls meet the defined requirements. If gaps are found, the R*equirements Definition* step itself will have to be revisited to address those gaps with additional requirements.

3.3 *Deliver Phase*

Now the policy can be implemented. The *Deliver* phase consists of two steps: *Controls Definition* and *Controls Implementation*.

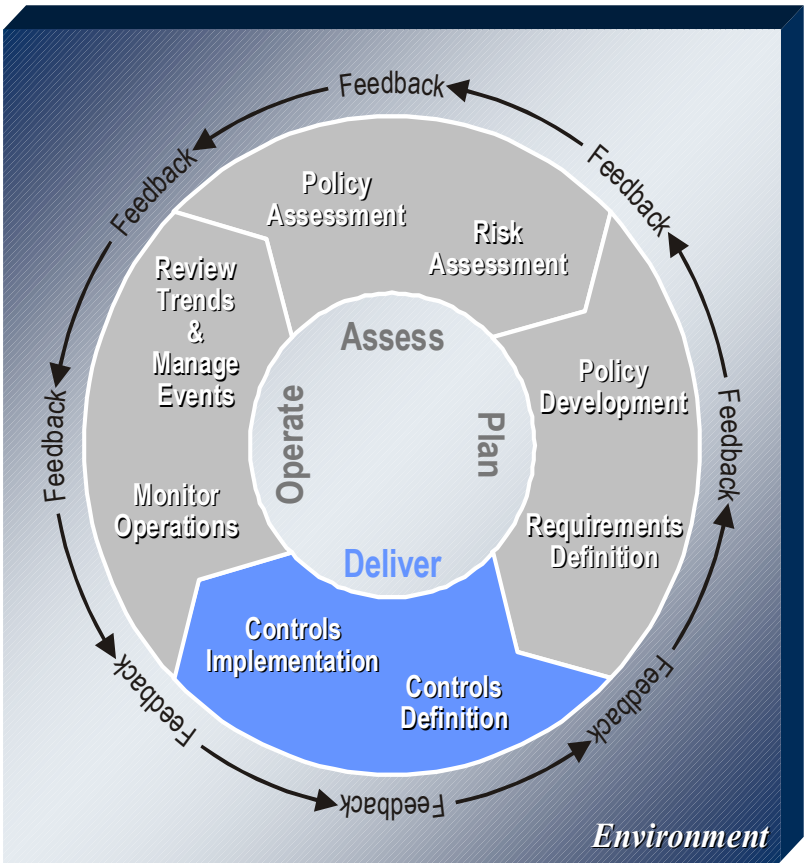

Figure 6: Deliver Phase

The outputs of the *Deliver* phase are:

- An implemented proposed change
- Complete standards, guidelines and procedures
- Complete security controls for the proposed change

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

3.3.1 Controls Definition Step

Controls are practices, procedures or mechanisms that reduce security risks, and this step defines those needed to meet the requirements of the security policy. In essence these controls form the security infrastructure -- technology, processes, and organizational security components.

3.3.1.1 Scope

The *Controls Definition* step is motivated by the necessity to accurately and efficiently fulfill the requirements set forth by the policy. Therefore its scope includes producing a specific implementation plan for the infrastructure to assure effectively building and configurating the necessary controls.

3.3.1.2 Step Methodology

Controls Definition consists of four sub-steps: Design Infrastructure, Determine Controls, Evaluate Solutions, and Select Controls. These sub-steps are sequential in nature and follow the widely-used software development life cycle (SDLC) [17].

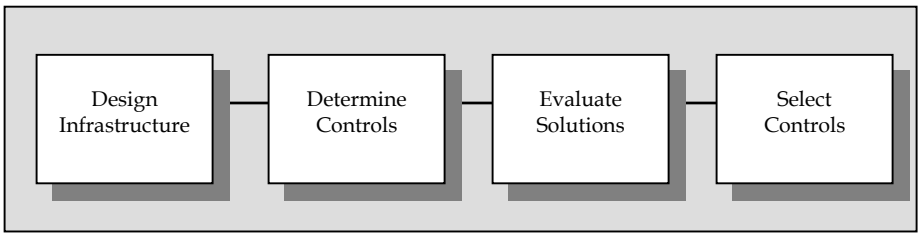

Figure g) Controls Definition Sub-steps

With his 23 years in the industry, the Nile.com CIO recognizes that all too frequently only technologists are put in charge of security infrastructure, rendering procedural and organizational issues easily overlooked. Therefore, he has convened a committee of both technical and non-technical individuals to take responsibility for defining controls.

Procedural design requires creating or modifying those procedures necessary to support the technical security infrastructure. It also includes creating or modifying business processes which require increased security. For example, with its move to online auctions, Nile.com must modify order processing procedures with an eye toward greater security.

Organizational design include creating or modifying a management structure for the security teams deployed as the policy matures. The newly-defined organization should include definitions of skill requirements and how process and procedure responsibilities should adapt accordingly. There may also be organizational impacts outside of the security team, such as increased responsibilities for system administrators and additional steering committee time for executives.

Copyright 1999, Andersen Consulting & CERIAS

3.3.1.2.1 Design Infrastructure Sub-step

In this sub-step, the requirements from the *Plan* phase are used to design a high-level security infrastructure containing technical, procedural, and organizational components.

The technical component will have several layers -- application, network, and operating system. Each layer will need controls to protect against different types of threats and to provide multi-layered protection. The key is to meet the following security principles:

- Identification -- the ability to identify participants in a system
- Authentication -- the ability to verify identification of system participants
- Authorization -- the ability to limit the scope of access to information resources for individual participants (users or processes)
- Confidentiality -- protecting the secrecy of information in storage, transit, or use
- Integrity -- providing assurance that information stored and processed cannot be altered accidentally or intentionally, and that information received has not been manipulated or corrupted in transit
- Availability -- providing assurances that the information resources will be available as expected and service levels can be met
- Non-Repudiation -- providing a mechanism to verify that a transaction has occurred

These principles can be implemented at any or all of these three layers, depending on the strength of the control needed.

Application layer controls will vary from application to application. However, reuse is possible and highly encouraged. For example, rather than requiring separate authentication for each application, Nile.com and many other eCommerce companies are leveraging a single source of authentication, such as a PKI or a WAC (Web-based Access Control), over several applications.

At the network layer, a network diagram is created or reviewed to provide for proper segmentation and traffic control. Typically organizations have at least three separate regions of their network: an untrusted zone (connected directly to the Internet), a semi-trusted zone (containing some publicly accessible resources), and a trusted zone (containing private resources). Network segmentation is achieved through a variety of mechanisms, including firewalls and routers. Organizations with more advanced architectures or more stringent security requirements may consider further network segmentation for specific needs. For example, Nile.com's research and development

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

facilities are segmented within a corporate trusted LAN. For more information on network segmentation and technical security architectures see [6].

The operating system layer requires advanced authentication and authorization controls for operating system level access. Some operating systems have built-in controls, therefore influencing platform choice. Otherwise they can be added to any platform through an add-on package.

The procedural component should include processes and procedures necessary to support the security infrastructure, as well as adding controls to business processes. For example, Nile.com's security infrastructure will require a process to add and delete users. Additionally, the company's business process that processes customer-to-customer auction payments will require additional controls at different monetary levels.

Some of the procedural design cannot be completed until individual controls have been selected and implemented, or until the business processes have been completely defined. Therefore, the importance of this sub-step is primarily planning to assure the right processes are considered even though the design is not complete.

Finally, the organizational component will include processes and procedures that support both the security infrastructure and the business architecture.

3.3.1.2.2 Determine Controls Sub-step

Next, the high-level designs created in the previous sub-step are translated into controls and their requirements. For example, Nile.com's network design will require segmentation between the semi-trusted and trusted zones. This segmentation must be able to allow only specific protocols and specific users to pass to the trusted zone, and it must support a specific authentication scheme to do that. These characteristics are used to define control requirements.

For each required control, it might be helpful to create a matrix that details the requirements each control must meet -- security characteristics, performance requirements, interoperability requirements, etc. Specific organizations may have additional requirements, such as a control provided by a partner-vendor or other preferred provider; in Nile.com's case its preferred provider is a portal web site with specific interoperability requirements.

3.3.1.2.3 Evaluate Solutions Sub-step

The security marketplace is growing rapidly, and it is likely that there will be several choices that meet general requirements. The purpose of this sub-step is to identify and evaluate the options for each control and select the best option. As evaluation occurs the relative importance of

each requirement should be considered. For example, Nile.com's requirement for interoperability is more important than performance, but for an online gaming company performance probably takes a higher priority.

Some organizations may choose to perform a two-phase evaluation, identifying a long list of possible solutions which is then narrowed to a short list of likely solutions. Items on the short list are then tested to determine the best solution. There are several good texts available on the process of evaluation and selection; see especially [37] and [3]. The outcome of this sub-step is a completed evaluation matrix, mapping each evaluated solution to each of the control requirements.

3.3.1.2.4 Select Controls Sub-step

Now the solution that best meets the control requirements is selected and mapped to the infrastructure design. This is a good time to check the list of selected controls against the security policy requirements and verify that all requirements are being met – an example of the feedback loop functionality of the PFIRES model. At this point the controls list should be validated to assure that duplicate requirements are not being met by different solutions (two different controls performing the same function) and will identify opportunities for controls reuse across the security infrastructure.

3.3.1.3 Human Performance Implications

During the *Controls Definition* step the new policy is integrated with the organization. Tools and processes necessary to implement it may require new behaviors and responsibilities. The Organizational "As-is" Assessment, along with the new policy and requirements, will help drive the development of organizational controls needed for a successful policy implementation.

Much human performance activity will be required to address both ability and motivation as key change factors. Training and performance support, as well as strong leadership and communication, are critical.

Specific training, communications, and human resources requirements will be refined at the same time as processes and technology are selected, but there will be a lag between processes and technology finalization and the human performance deliverables.

The following questions should be addressed:

- Do those in charge of security have the appropriate level of authority?
- Is responsibility for security linked to their performance review and compensation?
- Can the new policy be implemented given the size and competence

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

of the existing security organization?

- Are there sufficient training and communication resources to implement and support the new policy?

- What is the level of commitment to the new policy by each involved group?

By the end of the *Controls Definition* step, wide-spread acceptance of the new policy must be obtained in order to move forward with installing new controls and transitioning to new work processes. The communications effort begun during the *Assess* and *Plan* phases probably has obtained buy-in from users, so technical employees may already be at the Commitment stage [8]. Other stakeholders may only be at the Preparation or Acceptance phase [8]. As training gets underway and they work with the policy on a daily basis, however, they will advance.

Training regarding the new policy, as well as any new work processes or responsibilities, should be provided. Online performance support, self-study, or instructor-led training are some options available.

The installation of critical technologies and processes and deployment of the policy may trigger the need for new jobs and/or new roles and responsibilities for existing jobs. Assigning ownership for the various hardware and software involved in security may have implications for organizational structure in terms of levels of authority, reporting relationships, and staffing levels.

3.3.1.4 eCommerce Implications

Integration between controls is crucial in an eCommerce environment. In order for an eCommerce solution to integrate seamlessly multiple applications and information sources, the controls must be tightly integrated themselves. For example, Nile.com's applications share authentication information so the user is required to sign in only once. If each component has its own security component, the openness of the eCommerce solution is quickly lost.

3.3.1.5 Conclusion

By using the security policy to drive controls definition, the security infrastructure is uniquely designed to support the specific needs of the eCommerce solution. The threats that were identified can be easily mapped to the control device that minimizes them. Without a strong security policy, the *Controls Definition* step can become a random mixture of tools which are interesting but don't adequately protect the environment.

3.3.2 Controls Implementation Step

This step implements the controls selected in the prior step. Activities include building, testing, and implementing the final security infrastructure.

3.3.2.1 Scope

The scope of this step will vary widely depending on the controls. If the security infrastructure is being built from scratch to support a new business capability or market offering, as it is in Nile.com's case, then the *Controls Implementation* step may be very complex and last several months. If the security infrastructure is being slightly modified to adapt to a new threat, a few days may suffice.

3.3.2.2 Step Methodology

This step is executed through four sub-steps: Create Implementation Plan, Build, Test, and Pilot and Deployment. These sub-steps have some amount of overlap; Build will not be complete until Test has verified that it meets requirements. The infrastructure is typically piloted in a limited environment, then deployed to the organization; however, depending on the scope of the solution, a pilot may not be warranted. During deployment, once the infrastructure is in place in the "live" environment, a final risk assessment should be performed to assure that all known threats have been addressed and the solution is secure.

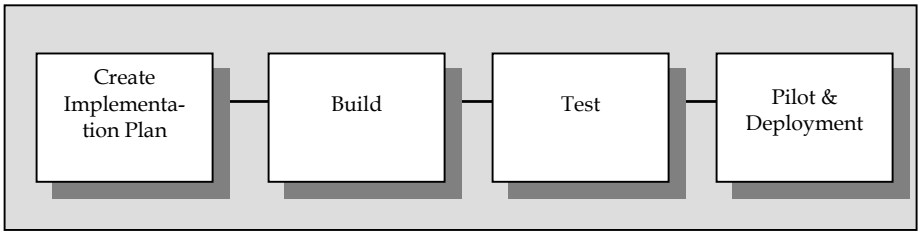

Figure h) Controls Implementation Sub-steps

3.3.2.2.1 Create Implementation Plan Sub-step

A specific plan is now necessary to translate design into reality. With a detailed plan, the security infrastructure is more likely to be built on time and to meet requirements.

Project planning methodology is available from several sources; see [39], [21] and [29]. A security infrastructure, however, has some specific requirements. Special attention should be paid to interaction points between the security architecture and the rest of the technical infrastructure. The plan should identify which areas will be affected, how they will be affected, and the anticipated time frames for deployment activities. Areas that might be affected at Nile.com, for example, include the help desk function, system administrators, network management, change management, and internal audit. The plan should

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

also consider how security will be maintained during the deployment or conversion process.

3.3.2.2.2 Build Sub-step

The scope of this sub-step will vary widely depending on the controls. If, as in the case of Nile.com's new market offering, the security infrastructure is being completely revamped, then the build sub-step may require several months. If the security infrastructure is being slightly modified to adapt to a new threat – say a new type of email virus -- then the build sub-step may be only a few days.

Thus the specific tasks for the build sub-step are not addressed in this document. Several resources are available with best practices on security infrastructure build; see especially [17].

But there are some specific planning considerations. It is in this sub-step where detailed procedures and performance support are developed to support the selected controls. These procedures are critical to the successful ongoing management and monitoring of the security architecture. This sub-step also includes activities to develop training products including help files and manuals.

Another planning consideration is to focus on building secure configurations that can be maintained once deployed. For example, Nile.com is migrating to a new operating system that will require some type of hardening. By creating automated scripts to do this, the company's security staff will find the configuration more easily updated and maintained.

3.3.2.2.3 Test Sub-step

Once the security infrastructure has been built, it must be tested to assure that the design was completely executed, that the identified threats have been addressed, and that no new vulnerabilities have been identified. Activities during this sub-step will include three types of testing: vulnerability assessment, security infrastructure validation, and application security support.

Vulnerability assessment validates that the new infrastructure has addressed all known threats and will identify new threats that have emerged since the design step. This testing should also include validating the infrastructure against the requirements originally set forth in the security policy. Vulnerability testing can follow the same methodology used during the *Risk Assessment* step of PFIRES.

Security infrastructure validation demonstrates that the infrastructure performs as intended, for example, that the intrusion detection tools are identifying the specified types of attacks and performing the appropriate notifications [11]. This testing activity also includes validating the procedures and human performance tools which support the security infrastructure. Because of the large scope of Nile.com's infrastructure

build, it will be appropriate to perform specific tests on each of the system components: Internet firewall, web server, application firewall, communications server, database server, host and network segments.

Application security support takes place in conjunction with application testing, assuring that the security infrastructure interacts appropriately with the supported business application. At Nile.com, for example, this would include user sign-on and access control. Test cases should be developed and executed in conjunction with the larger functional application testing team.

3.3.2.2.4 Pilot and Deployment Sub-step

Once tested, the security infrastructure is deployed to the production environment. Whether a pilot is required depends on scope. Of course, all changes large and small should be thoroughly tested before deployment, but that will have been accomplished in the previous two sub-steps.

Because of its large infrastructure change, Nile.com will conduct a pilot to identify any troublesome issues prior to a wide-scale deployment. The pilot will assure that the new business capability, e-auctioning, can be successfully and securely launched; all security risks will be evaluated and decisions made to either address or accept the risk. If risks are identified, the company will determine if activities are necessary to mitigate them and update the current security risk assessment accordingly.

Deployment includes configuring and installing security architecture components and rolling out new processes and procedures through communication and training. Deployment should ensure that security requirements as set forth in the policy are met, and that no new security risks are introduced. Specific tasks include configuring components to meet standards, verifying that configurations meet security standards, and performing a final security risk assessment on an appropriate scale. This might include security penetration testing or monitoring.

3.3.2.3 Human Performance Implications

It is during *Controls Implementation* that human performance solutions are implemented. Training is tested and delivered, more communications are rolled out, and new job(s)/role(s) are installed. There should be a lag between the completion of controls development work and the testing of training programs to limit rework of training programs due to changes in the controls.

Sponsor involvement must be public during this step. Communication from more senior members of the organization will increase the likelihood of acceptance by the organization as a whole and help promote individuals through the stages of commitment. At Nile.com, not only the CEO and CIO are publishing memos and sponsoring brown-bag lunches. Supervisors and department heads are also

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

discussing the changes so that people link the policy changes to their own job responsibilities. Additionally, policy-related responsibilities are being written into performance plans and departmental goals to assist monitoring and enforcement. As security responsibilities increase, compensation for security professionals is also increasing to retain valued human resources.

3.3.2.4 eCommerce Implications

The rapid deployment of eCommerce solutions requires equally rapid security infrastructure deployment. The challenge is to complete the necessary configuration and testing activities to assure the security of the solution in a relatively short implementation period.

Executives at Nile.com know that in the hypercompetitive world of eCommerce, the barriers to entry are very low and the possible rewards extremely high. That is why the introduction of its new business offering is scheduled to consume a mere three months from design to deployment. The executives also know that a rush to market brings with it the risk of a rush to judgment, so they have built in a security infrastructure from day one. Using PFIRES methodology allows Nile.com to build security policy concurrently, thus saving a great deal of time.

3.3.2.5 Conclusion

Controls Implementation is all about completeness. Prior steps have focused on defining an appropriate policy, determining requirements, and designing an infrastructure. This step takes all of that planning and translates it into action; therefore quality assurance and implementation integrity are especially critical. The security policy must be continually referenced to assure that its intent and requirements are met.

3.4 *Operate Phase*

The *Operate* phase of PFIRES occurs on a daily basis. Its purpose is to monitor the controls that have been put in place to secure the organization and handle incidents as they arise. In addition, business and technology trends are watched and analyzed.

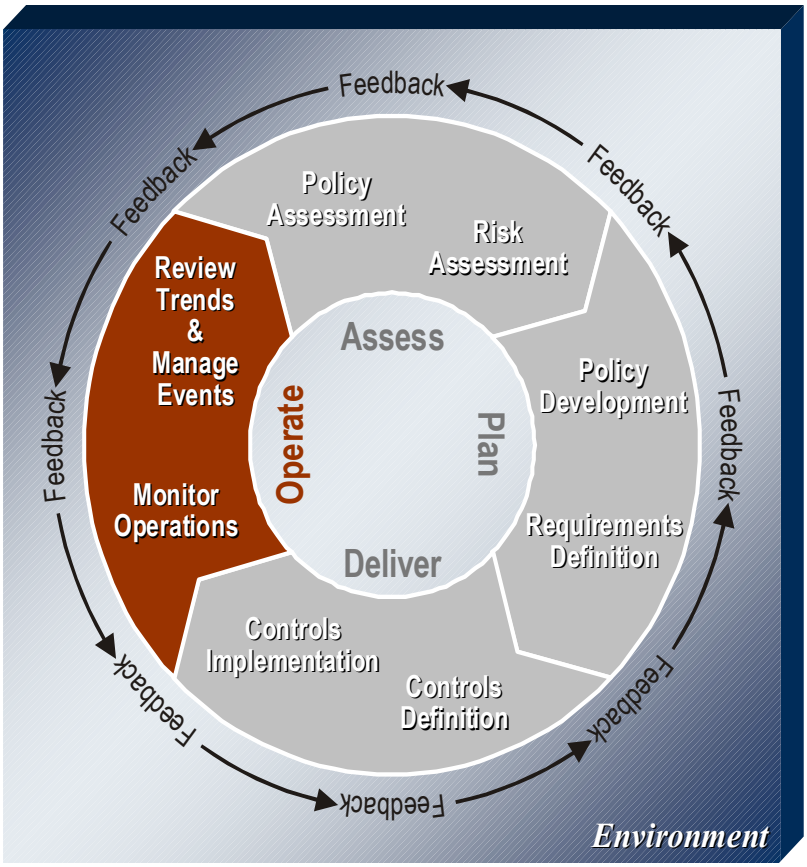

Figure 7: Operate Phase

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

3.4.1 Monitor Operations Step

The purpose of this step is to define the daily activities throughout the organization to ensure that the security policy is enforced across the security infrastructure. These activities can be broken into a few general categories:

Administration and Operations	Administer anti-virus software, common operating environment and workstation configuration policies, user accounts and access rules, operating systems, firewalls, remote dial-up access, backups
Security Services	Support teams and projects in the appropriate implementation of the security policy
Communication	Distribute alerts, deliver awareness program, provide security training
Investigation	Investigate intrusions, fraud, and errors
Compliance	Perform system audits and reviews, perform intrusion detection and penetration testing, perform user activity audit trail analysis; ensure compliance with internal standards and external regulations

3.4.1.1 Scope

There tends to be overlap between *Monitor Operations* and *Review Trends and Manage Events*, and the steps are not necessarily sequential. Often the organization will continue to operate normally while a team is investigating a particular event which may necessitate a security policy change. Therefore the entrance and exit criteria for these steps are not as clear as for other steps. Basically, *Monitor Operations* concerns planned activities necessary to support the security infrastructure and policy while *Review Trends and Manage Events* focuses on unplanned events.

3.4.1.2 Step Methodology

This step is unique because it is not clearly executed through a series of sub-steps. *Monitor Operations* consists of several simultaneous activities which must co-exist to support the environment.

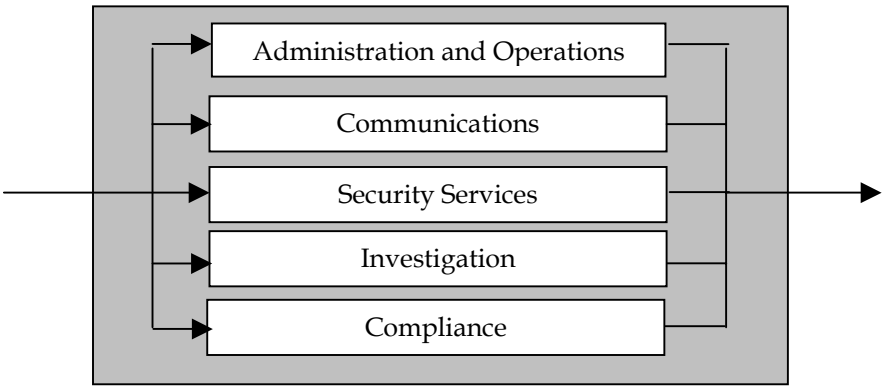

Figure i) Monitor Operations Concurrent Sub-steps

It should be noted that PFIRES does not address specific steps to support a security infrastructure or monitor a system; it is intended to address how a security policy should be used to drive the overall security efforts of an organization. There are several quality resources describing best practices of how to manage a security environment; see especially [14], [23], [18].

3.4.1.2.1 Administration and Operations Sub-step

This sub-step covers administrative functions and can include, but is not limited to:

- User administration (adding, deleting, and modifying system and application users)
- Evaluating and applying security patches to systems and applications
- System and application monitoring for security events
- Monitoring security news resources for new vulnerabilities
- Administering anti-virus applications

It is important to have a clearly defined role for each security administration/operation function. This role description should delineate the scope of responsibilities, performance measurement criteria, and required skills. It is also important that the individual in the role be given an appropriate amount of time and training. to execute the role and maintain skills.

In today's highly networked environment, the most diligent administrator is just as vulnerable as the most negligent. Therefore, it is also vital to have clearly defined procedures and processes for administration tasks, especially in a distributed environment where multiple people across an organization will be performing the same function for different user groups. For example, each of Nile.com's nine

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

physical office locations has one administrator responsible for security on the Unix servers at that office. Without defined procedures, each administrator could be handling one issue, such as patch management, differently.

3.4.1.2.2 Communications Sub-step

This sub-step communicates to different audiences the appropriate security messages. Each organization will have several different audiences, some requiring only an awareness of security, and others requiring time-sensitive information.

SAMPLE AUDIENCE	SAMPLE KEY MESSAGES
End-Users	• Protect your authentication credentials • Do not download material from unknown sources • Comply with Internet Acceptable Use policies
Unix Security Administrators	• Review recent CERT alerts on new vulnerabilities • Change security standards based on new threats • Installation procedures for tested security patches to install

A security infrastructure is only as strong as the individuals who maintain it. Therefore, time and attention must be paid to maximizing the human performance side of security. Specific planning considerations include:

- Think about how security will affect the way users do their job, and the type of support that users may require
- Communicate each individual's responsibility in protecting the confidentiality, integrity, and availability of information assets
- Develop a training plan for security architects, administrators, and analysts
- Use all available training modes and organizational mechanisms to facilitate the behavior changes necessary to improve security awareness

3.4.1.2.3 Investigations Sub-step

This sub-step includes those activities necessary to examine a situation or incident, determine root cause or verify facts, and recommend action. Common situations where an investigation will be necessary include:

- After a break-in or hack has occurred
- When an employee is suspected of violating corporate policy
- After an unplanned security event caused a system to crash
- After a fraud has occurred

In addition to strong technical skills to identify problems and determine causes, investigators may also need to be knowledgeable in legal issues to assist in building a prosecutable case. Of course, investigations rarely occur on a daily basis so it may not be necessary to staff this function full-time; at Nile.com, investigations is a component of an incident response team with other full- and part- time roles. (See the *Incident Response* sub-step *in Review Trends and Manage Events*.)

3.4.1.2.4 Security Services Sub-step

Outwardly this sub-step may seem identical to security administration, but there is a clear delineation between the two. Security services deals with providing security specialists to project teams as they design new capabilities, refine existing processes, or otherwise undertake change within the environment.

For example, along with its corporate strategic makeover, Nile.com's small procurement business unit is interested in migrating remote access for their application from dial-up to Internet. They have an application support team already in place to make the transition, but no one is sure of the security implications. The security services team is providing a resource on a part-time basis for the duration of the project to identify increased application security requirements and integrate the application into the existing web security architecture.

The security services function can be viewed as a consulting role and can be filled by a dedicated group within the security organization or by an external service provider.

3.4.1.2.5 Compliance Sub-step

This sub-step includes those activities necessary to ensure the infrastructure is following security policy guidelines. It is typically thought of as an internal audit function, but a security compliance program is more proactive than quarterly audit reports and findings. Security compliance activities include:

- Procedures that outline activities administrators and operators should perform frequently (e.g., weekly) to monitor their own compliance

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

- Tools that enable the consistent compliance of tools to the security policy (e.g., all NT servers meet a minimum baseline of security requirements)

- Monitoring user activity through audit trail analysis

- Considering both internal and external regulations for compliance procedures.

For effective compliance there must be a combination of proactive compliance on behalf of the administrators/operators/service providers, and scheduled reviews by the compliance enforcement team.

3.4.1.3 Human Performance Implications

Once implementation is complete it is important to monitor adherence to the new policy and procedures. The organization should be looking at how well the policy is meeting its needs, whether people are willing and able to adhere to the policy given their knowledge skills and work processes, and whether there are any environmental or strategic changes that could trigger a new proposed change through the life cycle.

In this step, human performance is most concerned with how to support personnel in using the policies, standards, guidelines, and procedures that have been developed. At Nile.com, intrusion detection systems as well as audits, supervision, and measurement are all tools used for monitoring. Additionally, the company provides ongoing communication and performance support; these are effective ways to continually engage personnel in thinking about their role in security and to appreciate the need for frequent change given the dynamic eCommerce environment. The communications and training plans and deliverables should be transitioned a team to support and maintain them during the lifetime of the policy.

3.4.1.4 eCommerce Implications

Execution of security policy in an operational environment becomes more critical in an eCommerce environment for two reasons:

- eCommerce requires an ever-increasingly networked environment, across all business units and locations. In that internetworked system, security is only as strong as the weakest point, so operational quality and compliance vital to reduce the global risk to an organization.

- Execution of security policy can help identify deficiencies in security policy. For example, Nile.com's current security policy states that no mobile code technology can be downloaded from the organization to the user. But a compliance review in the future may discover that an application has enabled some great new functionality by allowing mobile code downloads. This discovery may then trigger a review of that policy element, and a subsequent trip through the PFIRES life

cycle.

3.4.1.5 Conclusion

If the security policy was written effectively, adhered to closely during the life cycle, and continually re-evaluated at each step for feedback, the *Monitor Operations* step will provide the right level of security for the organization. Of course, there are a lot of unknowns, and during this step organizations will likely identify a new threat that wasn't considered, a new technology that's needed, or a business capability that was forgotten.

It is in these situations where the life cycle model is most appropriate, because the organization is uniquely situated to take a quick tactical pass through the life cycle to address the situation.

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

3.4.2 Review Trends and Manage Events Step

A security policy that is not constantly evaluated and updated is of no value. This step identifies those events or trends that may signal a need to re-evaluate the security policy.

3.4.2.1 Scope

The scope of this step includes reviewing existing security controls for their effectiveness, reviewing security policy exception cases, and reviewing internal and external information sources and evaluating their effect on the security policy. This step does not include the actual decision whether to change the policy, and the scope of that change, both of which are the result of the *Assess* phase.

This step also manages events identified during the *Monitor Operations* step. If there are procedures to handle these events, those procedures are executed. If the event is larger in scope than can be managed in this step, the life cycle shifts into the *Assess* phase. As an example, if Nile.com discovers a major security flaw in a mission critical application that standard event management procedures could not take care of, a pass through the PFIRES life cycle would be appropriate.

3.4.2.2 Methodology

This step can be broken down into the following four sub-steps:

- Manage events (planned and unplanned)
- Identify internal trends
- Identify external trends
- Escalate to *Assess* phase

As in the *Monitor Operations* step, these activities are not executed sequentially. Although escalation is always the last step, event management and trend identification can take place at the same time.

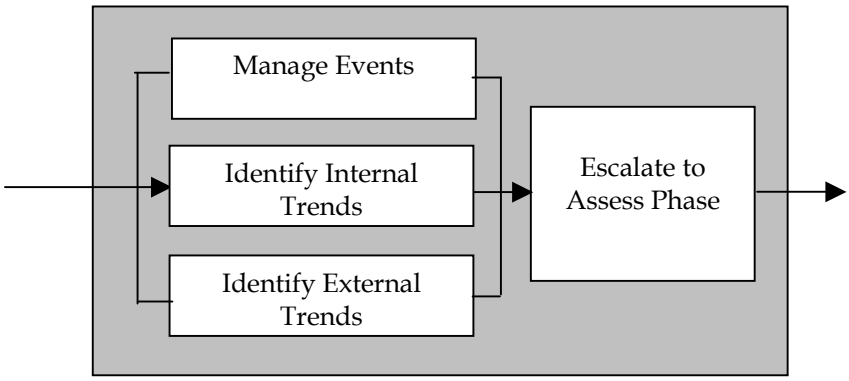

Figure j) Review Trends and Manage Events Concurrent Sub-steps

3.4.2.2.1 Manage Events Sub-step

As used in this context, events are situations or circumstances outside the boundaries of normal activity, for example, an individual violating an acceptable use policy. Nile.com's policy states that employees may not surf sports sites during work hours. But an audit log shows an individual doing just that. Although outside of normal or expected activity, it is a likely event which can easily be planned for. Therefore, procedures can be put in place so if and when it does occur it can be processed as part of planned operations. Nile.com procedures dictate that the employee's supervisor reprimand him and places a notice in his personnel file.

On the other hand, there are situations or circumstances which cannot be planned for -- unexpected events like fraud or destruction of data. Specific management procedures cannot be anticipated for each event. Rather, they require an incident response process.

The incident response process is defined during the *Controls Implementation* step, and these response procedures must be in place to assure events are handled effectively during the *Review Trends and Monitor Events* step.

Incident response processes must include the following activities: [15]

- Documenting actions taken during the incident
- Maintaining records of what was altered during the incident
- Providing appropriate information to support legal action
- Procedures for tracing the source of an event
- Guidelines for when or how to escalate an event through chain of management
- Procedures for containment of events to limit damage

In addition to these basic procedural issues, event management has additional considerations:

- A designated team should be responsible for executing the incident response process. This team must have an appropriate mix of technical -- network and operating system -- skills to be able to track and mitigate an event as well as application-specific skills for high-risk business applications. Because responding to incidents will not be a full-time job for most organizations with a well-defined security policy, team members can come from everyday roles within the organization (e.g., system administrators, technical department heads, etc.).
- Specific technologies can be valuable in both identifying an event and in managing that event after identification. For example,

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

Nile.com intrusion detection tools alert an operator if certain thresholds are exceeded. Additionally, the company has network tracing tools to use to track the origin in the event of an attack.

- Events will have different levels of priority and should be managed accordingly. Typically change requests for new access to systems are relatively low priority compared to reports of downtime of an authentication service.

3.4.2.2.2 Identify External Trends Sub-step

This sub-step looks for external trends that may indicate the need to reassess current security policy. Its key components are: identifying information which may have security relevance and determining whether to escalate a trend or event to the *Assess* phase.

Both business and technical trends should be monitored. Technical trends include advancements in technologies that application developers will want to leverage and that security policy must adequately protect. Among business trends, the abandonment of vertical markets as more companies outsource non-core business functions adds a potential security requirement to open internal systems to a third party.

To determine if an event or trend should be escalated, it must be looked at within the context of the organization's industry, and should also be evaluated in terms of organizational priorities. For example, competitive intelligence (CI) professionals within Nile.com have noticed a trend among e-auction houses to promote the sale of dubious items such as human organs for transplantation. To the CI group, the legal and ethical implications of this trend are obvious, but the security ones are not, so they've passed it along to the director of security for further investigation.

When identifying external trends, some additional items should be considered:

- Sources of information should be identified and assigned for review. Nile.com interns scan sources such as CERT (Center for Emergency Response Teams, http://www.cert.org) daily for new vulnerabilities. They also peruse industry and analyst reviews and user conference proceedings less frequently to identify visionary thinking within the industry.

- Advanced technology may be used to discover "hidden" trends; Nile.com has employed data mining, for example, to drill external data sources and web farming to automate web search and analysis.

3.4.2.2.3 Identify Internal Trends Sub-step

Internal trends can come from new business opportunities, new capabilities, or new applications. Or they may arise from an existing business or security process.

New opportunities may be easier to identify. At Nile.com it something new was clearly on the horizon when the vice president of sales began to request new hardware, software, and applications to support the company's strategic e-auctioning move. Changes such as these should go through the organization's change control process for approval before becoming a proposed change. If a request becomes a proposed change, it will be escalated to the *Assess* phase of the model. A security representative should be part of the organization's formal change control process so that the security implications of these requests are identified and considered.

Trends within current processes may be harder to notice. In the *Controls Implementation* step, monitoring and reporting mechanisms will be put in place to collect and collate data. This data should then be summarized to report on key performance indicators: e.g., the number of violations of the Internet Acceptable Use policy, or number of attempted and refused telnet connections. Patterns in this Key Performance Indicator (KPI) can then identify a need for a change.

For example, Nile.com's weekly firewall report includes information on the number of attempted outbound ftp (file transfer protocol) requests which were rejected. By comparing these numbers with the expected average and threshold values, a report reviewer can note excessive rejections; if three weeks go by where values exceeded Nile.com's threshold, that would constitute a trend.

The trend must be looked at in context, of course. The reviewer must take into consideration information such as the network segment initiating the requests and the destination site. A Nile.com development team trying to ftp from a software vendor's web site is a different case than a help desk team workstation trying to ftp from a joke web site.

3.4.2.2.4 Escalate to Assess Phase Sub-step

Not all changes should be escalated to the *Assess* phase -- common sense and a set of criteria should prevail. These criteria need not be pages of detailed considerations, but they should validate a true impetus for change.

These key issues should be examined:

- Scope of impact. Will this change impact a single business unit or group within the organization, or will it have a global business impact?
- Timeliness. Has the need for this change been proven over time?
- Momentum. Is there support among key stakeholders (system administrators, application owners, business unit leaders) that this change is necessary?

Examining these factors and providing context around the proposed

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

change, the *Review Trends and Monitor Events* step will conclude with a more accurate decision.

3.4.2.3 Human Performance Implications

Now human performance can turn its attention to reviewing the outcomes of the implemented change against the gaps identified in the Organizational "As-is" Assessment. If it is found that gaps identified were not successfully addressed, these can become proposed changes to be promoted into the *Assess* phase and through the life cycle.

3.4.2.4 eCommerce Implications

A key consideration of eCommerce is always the pace of change. Technology that is hot today was not even invented two years ago. Security vulnerabilities that are easily prevented today were undetectable a short time ago. This step is where these trends in technology and security and business are continually scanned to ensure an effective security policy.

3.4.2.5 Conclusion

Change is good. An overused cliché, maybe, but in today's mercurial eCommerce environment, change is necessary to survival. A security policy that doesn't adapt will become obsolete and the organization it used to protect, perhaps extinct. The PFIRES life cycle embodies the ongoing process of adaptation and evolution needed to create a security policy that can keep up.

4 Conclusion

There are many products, tools, and procedures for managing information security, but none for managing security policy. These tools are fine in and of themselves, but if not organized around a solid security policy they are tools that will likely fail. PFIRES is a different kind of tool, one for high-level management of an organization's information and financial assets related to eCommerce – its security strategy and policy.

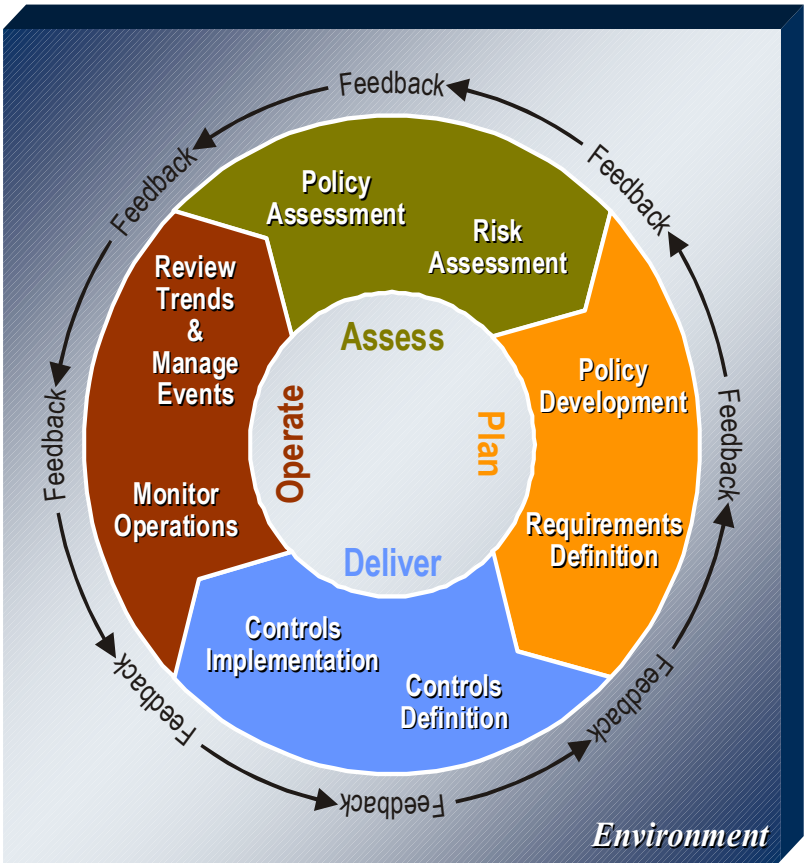

Figure 8: PFIRES Life Cycle Model

PFIRES's unique approach emphasizes change in the organization's operating environment as the driver of life cycle activities. By allowing environmental change to drive life cycle activities, the organization can assume a more proactive rather than purely reactive role in managing its security infrastructure. PFIRES also recognizes a continuum of change -- strategic to tactical – providing relevant guidance for managing change in every shade of gray.

As a high-level policy management tool PFIRES facilitates communication between senior management and technical security management. With improved communication the organization should

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

realize immediate benefit -- increased protection from and responsiveness to security incidents related to eCommerce activities. By effectively managing security risks, the organization is better positioned to successfully achieve its eCommerce objectives.

Much work remains to be done in this area. International and regional concerns, organizational behavior, legal issues, supply-chain, and industry-specific concerns are a few areas that would benefit from an in-depth exploration of related information security policy. Enhanced models and tools for analyzing and managing information security infrastructure investments are also needed. Certainly, research needs to be conducted into how well the life cycle meets the policy management needs of today's organizations and what improvements need to be made to ensure future success.

5 Appendix

5.1 Assessing the costs of security breaches : The modified ALE model

Introduction

While the need for a security policy for eCommerce activities is not in dispute, as is the case for other IT infrastructure investments, it is useful to provide cost-justification for the investment. Some methods do exist for assessing the costs of security breaches, but given the complex nature of the problem, it is difficult at best to quantify the full extent of a security breach in monetary terms. For example, a recent 22 hour outage at the popular Internet auction site illustrates the complexity of the problem: in an eCommerce world, production outages of less than a day (that would be hardly discernable in the pre-Internet era) can mean handsome gains for competitors (the auction sites of Amazon and Yahoo! reported a steep increase in trading and new registrations that day and after), as well as long-term losses (eBay announced that it will have no transaction charges for the outage period, which translated into a loss of revenues of nearly $5 million, and a consequential fall in eBay's stock price by nearly $30). While such incidents will definitely occur in future, it is impossible to estimate the extent of the damage caused by the incident - or predict such an incident in advance.

The following is a synthesis of the research in this area to develop a model (called the modified ALE model) that is suitable for use in the business environment. However, it is prudent to remember that formulas and numerical assessments of risk, while seemingly objective, are just tools to help the security team arrive at its final assessment. If project team members use these methods and arrive at conclusions that do not seem reasonable, they should either re-examine their initial assumptions or consult a security practitioner with more experience.

The model estimates the frequency of various types of security breaching incidents and the costs involved in bringing the system back to the state it was in before the incident. The annual cost of a particular type of an incident can then be estimated from these data.

The ALE model

There are few methods available today that quantify the effects of a security breach. For any organization investing in a security policy, this lack of usable tools is problematic. The first step in justifying a security investment decision is to know in quantitative terms what we are protecting against. The widely known Annual Loss Expectancy or the ALE model, while simple to understand, is not easy to use. The Annual Loss Expectancy (ALE) [1] can be represented by the following formula:

$$ALE = p * c$$

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

Where

P = the probability that a threat will take place during one year

C = the cost to the organization if the threat occurred, including direct replacement of assets and consequential costs arising from loss of business

While simple and intuitive to understand, both parameters p and c are difficult to estimate. We suggest a methodology, which we call the modified ALE methodology, to estimate the cost of security breaches to an organization. This is partially based on the *Incident Cost Analysis and Modeling Project* (ICAMP) [34].

Estimating the frequency of an incident

One way to estimate the probability of a security breach is to results of recent security surveys [5], [10], [31]. One survey provides reports of the frequency of various types of security breaches. While such figures should provide some initial estimates, it might be advisable to measure the frequency of various types of threats for a particular organization. The major types of security breaches, as noted in [5] are viruses (77%), employee abuse (52%), unauthorized access by outsiders (23%), theft/destruction of computing resources (23%), leak of proprietary information (18%), theft/destruction of data (15%), access abuse by non-employee authorized users (14%) and hacking of phone/PBX (12%). These classifications may be used by an organization internally to categorize their own set of security breaches, and the frequency of each could be noted over a period of three months. These frequency measures could be used to estimate the number of security breaches of each type annually.

Estimating costs of an incident

To estimate the cost of each type of security breach, we use a methodology similar to the ICAMP [34]. The cost of a breach is the sum total of all expenses required to bring the system to its original state before the breach. Note that this measure of costs will likely underestimate the actual costs to the organization, since it does not take into account some of the opportunity costs to the organization that are difficult to measure. For any sort of security breach, there can be four kinds of associated costs: IT employee costs; external and internal consultant costs; user costs; and new purchases required to return the system to its original state. We discuss each of these costs briefly.

IT employee costs: These are the costs of the various employees of the IS department who are engaged to bring the system back to its original status. The employees include data entry operators, programmers, system administrators, and others. The IT employee costs are reflected in their wages times the number of hours spent by each in the recovery operation. As there exists a possibility of error in recalling past events, the wage costs are calculated within a confidence interval of 15%, as in

the ICAMP project. Given the uncertainty in the data collection, this is a necessary procedure.

The actual calculation involves dividing an individual's wage by 52 weeks per year and 40 hours per week to obtain an hourly wage (the calculations are suitably modified for those employees on monthly salaries). The wages should include all benefits to the employees: one way to compute benefit costs is to estimate the average benefits as a percentage of salary, obtaining required data from Human Resources. There are other indirect costs to an organization for an employee, details of which can again be obtained from the Human Resources department. For a particular incident, the number of hours spent by each category of employees is estimated, and then multiplied by the hourly rates to estimate the IT employee costs. The +/- 15% interval gives an estimate of the extent of variation of the figures in the individual incidents of breach.

Consultant costs: Incident resolution often requires the assistance of a technical consultant. The fee charged by the consultant is to be used as the real cost.

User side costs: During the investigation and analysis of an incident, the user costs are difficult to estimate. User costs consists of costs borne by the clients of the affected system due to malfunctioning equipment, lost or inaccurate data, disclosure of sensitive information, denial of service, etc. Any time a user cannot access a service that she needs to perform any business function, or has to restore data, a cost is associated with the wasted time.

The difficulty lies in assessing the cost of the wasted time, since it is impossible to say for certain what a user's time is worth. This includes not only her wages, but also opportunity costs that cannot be easily quantified. Also, it is impossible in most cases to speak to every affected user. Thus, estimating the user costs based on the available wage information will almost always underestimate the actual costs.

New purchases: If new hardware or software is required to bring the system back to its original state (e.g., a high speed scanner with optical character recognition (OCR) software to re-enter lost data, or a software imaging solution), the purchase price should be included as cost of the incident. If the purchase of some new equipment is expedited the incident, but was otherwise previously planned for, then the costs of such equipment cannot be considered as part of the incident's cost.

An added consideration for equipment costs is that they are often *not* repeated after the first incidence. Therefore, care must be taken to amortize these costs across all instances of an incident.

Opportunity costs: If some costs can be directly attributed to the incident (e.g., loss of sales revenue from the eCommerce activities due to the site being down for a few hours, or, compensating affected customers during disruption of services), they should be included as part of the incident's cost. In general, any loss of revenue or increase in costs of running the

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

business that can be directly attributed to the incident should be considered as costs of the incident.

All the above data capture only the costs than are quantifiable. In many cases, a significant component of the actual costs of an incident might be non-quantifiable. Some of these costs are the reputation of the company (which might have long-term profitability implications), loss of investor and customer confidence, etc. There are also incidents that have not yet occurred whose costs cannot be estimated for this model (since this model depends on data from past incidents). Future research will address such issues to enable policy planners with a more robust tool for estimating the true cost of security breaches.

Calculating the costs of the incident

The various cost data about the users, the IT employees, consultants, and other components of the incident costs can be logged in a generalized spreadsheet as shown in below.

SAMPLE INCIDENT COST SPREADSHEET

IT Employee Costs					
Title	Logged hours	Hourly wage	Total	-15%	15%
Subtotal					
Benefits @X%					
Indirect cost rate Y%					
Total IT Employee Costs					
User Costs					
Title	Estimated hours	Value of time	Total	-15%	15%
Total User Costs					
Consultant costs					
	Logged hours	Hourly wage	Total	-15%	15%
Total Consultant Costs					
Equipment costs					
Hardware Software					
Total Equipment Costs					
Direct attributable costs					
Lost sales revenues Compensation to customers Communication expenses *Regulatory agencies* *Shareholder and financial*					
Total attributable costs					
TOTAL COSTS					

Determining the total costs per category of incidents per year

The above spreadsheet helps us to find the cost of a particular type of incident, by investigating the details of a particular incident of that type. The +/- 15% gives us an estimate by which the actual costs of other incidents might vary, though some judgment needs to be exercised in each case to determine whether the particular incident investigated is *typical* or not. This is extremely important, and it calls upon the experience of the policy makers to distinguish between a typical incident and an atypical one.

The total number of each type of incident per year can be estimated as follows:

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

Estimated number of security breaches of a particular type = Total number of security breaches per year (estimated from data from three months) * frequency of the particular incident (from internal estimates or from survey results)

This number can be multiplied by the cost of a typical incident of a particular type to arrive at the total costs per incident type per year. The total cost of all information security breaches is the sum of costs of all types of incidents arrived in the above fashion.

An example

The example below is fictional, but it serves to illustrate the above procedure. It considers the effect of the recent well-publicized CIH virus that affected corporate PC networks. We consider four types of likely costs:

- IT employee costs, incurred by the various people in the IS department involved in getting the PCs (or their replacements) back to full usability status.
- Recovery costs of the data lost due to the virus attack.
- Consultant costs, in terms of the external consultant who was called in to help resolve the problem.
- Equipment costs, which includes the cost of replaced hardware, software fixes and new software.

The IT employee costs and the consultant costs are estimated from the direct hours billed by the various people involved in the recovery.

As is evident from the example, it still underestimates the real costs, since in all probability, the incident would have had some opportunity costs, like lost revenues, etc.

SAMPLE INCIDENT COST: CIH VIRUS EXAMPLE

IT Employee Costs					
Title	Logged hours	Hourly wage	Total	-15%	15%
Technical analyst 1	16	$45.00	$720.00	$612.00	$828.00
Technical analyst 2	20	$45.00	$900.00	$765.00	$1,035.00
Technical analyst 3	14	$45.00	$630.00	$535.50	$724.50
Technical analyst 4	12	$45.00	$540.00	$459.00	$621.00
Technical analyst 5	25	$45.00	$1,125.00	$956.25	$1,293.75
Senior Analyst	20	$52.00	$1,040.00	$884.00	$1,196.00
Data entry operators (10)	80	$25.00	$2,000.00	$1,700.00	$2,300.00
Sr. Mgr. Network Services	8	$55.00	$440.00	$374.00	$506.00
Associate Director, IT	8	$65.00	$520.00	$442.00	$598.00
Subtotal			$7,915.00	$6,727.75	$9,102.25
Benefits @28%			$2,216.20	$1,883.77	$2,548.63
Indirect cost rate 52%			$4,115.80	$3,498.43	$4,733.17
Total IT Employee Costs			$14,247.00	$12,109.95	$16,384.05
Recovery Costs					
Recovery Items	Estimated hours	Value of time	Total	-15%	15%
Accounting system	100	$35.00	$3,500.00	$2,975.00	$4,025.00
Inventory Database	20	$35.00	$700.00	$595.00	$805.00
POS Data	10	$35.00	$350.00	$297.50	$402.50
Sales bonus data	5	$35.00	$175.00	$148.75	$201.25
Purchase orders	5	$35.00	$175.00	$148.75	$201.25
Directory structure	40	$35.00	$1,400.00	$1,190.00	$1,610.00
Session scripts	1	$35.00	$35.00	$29.75	$40.25
Problem log	3	$35.00	$105.00	$89.25	$120.75
Address directory	15	$35.00	$525.00	$446.25	$603.75
Total User Costs			$6,965.00	$5,920.25	$8,009.75
Consultant costs					
	Logged hours	Hourly wage	Total	-15%	15%
	20	$200.00	$4,000.00	$3,400.00	$4,600.00
Total Consultant Costs			$4,000.00	$3,400.00	$4,600.00
Equipment costs					
Hardware			$4,500.00	$3,825.00	$5,175.00
Software			$4,000.00	$3,400.00	$4,600.00
Total Equipment Costs			$8,500.00	$7,225.00	$9,775.00
TOTAL COSTS			$33,712.00	$28,655.20	$38,768.80

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

5.2 Glossary

Access Control – Techniques for controlling access to sensitive files.

Asset – Everything critical to the business including all forms of information or data, plus the people and technology that support information processes.

Authentication - A process used to verify identification of system participants.

Authorization -- The ability to limit the scope of access to information resources for individual participants (users or processes).

Availability -- Providing assurances that the information resources will be available as expected and service levels can be met.

Bandwidth – Measurement of the amount of data that can be send through a connection.

Biometrics – Authentication techniques that utilize the analysis of a person's physical characteristics, such as fingerprints, speech, and retina scans.

Certificate Authority – An entity authorized to issue security certificates that contain information about eCommerce players to allow secure online transactions.

Confidentiality -- Protecting the secrecy of information in storage, transit, or use.

Cryptography – The process of concealing the contents of a message from all except those who know the key.

Digital Signature - An encryption mechanism used to guarantee the authenticity of a message or file.

eCommerce - Commercial exchanges of value between an enterprise and an external entity, either an upstream supplier, a partner, or a downstream customer over a universal, ubiquitous electronic medium.

Encryption - The process of transforming data into a complex code so that it cannot be recovered without using a decryption process.

Extranet - A private network that uses the Internet protocols and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.

File Transfer Protocol (ftp) – The simplest way to exchange files between computers on the Internet.

Copyright 1999, Andersen Consulting & CERIAS

Firewall - A system or combination of systems that enforces a boundary between two or more networks.

Human Performance – The system of people, management, business environment that performs business processes.

Identification -- The ability to identify participants in a system.

Internet - A publicly accessible electronic medium typically used for consumer-oriented transactions, though also used for business-to-business transactions.

Internet Service Provider (ISP) - Entity which provides access to the Internet.

Infrastructure - The physical hardware used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, cable television lines, and satellites and antennas, and also the routers, aggregators, repeaters, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals that are transmitted.

Intrusion Detection - Techniques that attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data.

Non-Repudiation -- Providing a mechanism to verify that a transaction has occurred

Password - Confidential authentication information, usually composed of a string of characters used to provide access to a computer resource.

Public Key Infrastructure (PKI) - The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

Risk – The possibility of suffering harm or loss. In the context of information, risk involves danger to network infrastructure and data, and to the entire business operation.

Router – A hardware interface that finds the best route between networks.

Security Controls - A practice, procedure or mechanism that reduces security risks.

Security Guideline - Specific recommendations to address an element of the security policy.

Security Infrastructure –The people, process and technology controls that combine to create a secure solution.

Copyright © 1999 Andersen Consulting & CERIAS.
All Rights Reserved.

Security Policy - A high-level statement that describes management direction and support for information security focusing on the objectives of the corporate security program. Security Policy encompasses Security standards, guidelines and procedures.

Security Procedure - Specific actions required to implement security policies, standards and guidelines.

Security Standard - Specific, mandatory requirements to address an element of the security policy.

Security Strategy - An overview of future business directions and the security controls which should be in place to support these business functions.

Smart Card – A plastic card about the size of a credit card with an embedded microchip that can be loaded with data including a unique identification code.

Streaming Audio – Sound that is played as it arrives. The alternative is a sound recording (such as a WAV file) that doesn't start playing until the entire file has arrived.

Transaction - An electronic transfer of business information which consists of specific processes to facilitate communication over global networks.

6 References

[1] Bernstein, T., Bhimani, A. B., Schultz, E. and C. A. Seigel, *Internet Security for Business*, Wiley NY, 1996

[2] Bhimani, A., "Securing the Commercial Internet," *Communications of the ACM*, Vol. 30, no. 6, 1996, pp. 29-35.

[3] Boer, F.P., *The Valuation of Technology : Business and Financial Issues in R&D*, NY, John Wiley & Sons, 1999.

[4] Bond, R. and Whiteley, C., "Untangling the Web: A Review of Certain Secure E-Commerce Legal Issues," *International Review of Law, Computers and Technology,* Vol. 12, 1998.

[5] Briney, A., "Got Security?" *Information Security*, July, 1999, pp. 20 – 41.

[6] Comer, D. E., *Computer Networks and Internets*, Prentice Hall, Upper Saddle River, NJ., 1997.

[7] Computer Science and Telecommunications Board, "Trust in Cyberspace," Ed. F. B. Schneider, National Research Council, 1998.

[8] Conner, D. R., Managing at the Speed of Change: How Resilient Managers Succeed and Prosper Where Others Fail, Random House, NY, 1992.

[9] Dalton, G., "Acceptable Risks," *InformationWeek*, August 31, 1998, pp. 36-48.

[10] Ernst & Young LLP, "5th Annual Information Security Survey," http://www.ey.com/publicate/aabs/isaaspdf/FF0148.pdf, 1999.

[11] Escamilla, T., Intrusion Detection, Network Security Beyond the Firewall, John Wiley & Sons, Inc, 1998.

[12] Flaatten, P. O., et al., *Foundations of Business Systems*, The Dryden Press, Fort Worth, TX, 1991.

[13] Galpin, T. J., The Human Side of Change: A Practical Guide to Organizational Redesign, Jossey-Bass, San Fransisco, CA, 1996.

[14] Garfinkel, S. and Spafford, E., *Web Security & Commerce*, Cambridge, O'Reilly & Assoc., 1997.

[15] Guttman, B. and E. A. Robach, *An Introduction to Computer Security: The NIST Handbook*, National Institute of Standards and Technology, 1995.

[16] Heuss, E. *Allgemeine Markttheorie*, Tubingen, J. C. B. Mohr (Paul Siebeck), 1965.

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.

[17] Hoffer, J. A., George, J. F., and J. S. Valacich, *Modern Systems Analysis and Design,* Addison-Wesley, Reading, MA., 1999.

[18] Hutt, A.E., Bosworth, S., and Hoyt, D.B., *Computer Security Handbook*, NY, John Wiley & Sons, 1995.

[19] *Information Security Magazine*, July 1999.

[20] Kano, N. "Miryoku-teki Hinshitsu to Atarimae Hinshitsu," (in Japanese) *Journal of Japanese Society of Quality Control*, Vol. 14, no. 2.

[21] Kerzner, H., Project Management : A Systems Approach to Planning, Scheduling, and Controlling, NY, John Wiley & Sons, 1997.

[22] Kluepfel, H. M., "Securing a Global Village and Its Resources," *IEEE Communications Magazine,* Vol. 32, 1994.

[23] Krause, M. Tipton, H.F., *Handbook of Information Security Management*, NY, Auerbach Publications, 1999.

[24] Lichtenstein, S., "Developing Internet Security Policy for Organizations," *Proceedings of the Thirtieth Hawaii International Conference on Systems Sciences*, Eds. J. F. Nunamaker, Jr. and R. H. Sprague Jr., IEEE Computer Society, 1997, pp. 350-357.

[25] Magaziner, I. C., "The Framework for Global Electronic Commerce: A Policy Perspective," *Journal of International Affairs,* Vol. 51, 1998.

[26] Mayfield, W. T., Ross, R. S., Welke, S. R. and B. Brykczynski, "Commercial Perspectives on Information Assurance Research," Institute for Defense Analyses, 1997.

[27] Oliver, R. W., "Corporate Policies for Electronic Commerce," *Proceedings of the Thirtieth Hawaii International Conference on Systems Sciences*, Eds. J. F. Nunamaker, Jr. and R. H. Sprague Jr., IEEE Computer Society, 1997, pp.254-264.

[28] Oppenheimer, D. L., Wagner, D. A. and M. D. Crabb, *System Security: A Management Perspective*, The System Administrators Guild, 1997.

[29] Pennypacker, J.S. and Adams, J. R., *The Principles of Project Management*, Project Management Inst Pubns, 1997.

[30] Porter, M. E., Competitive Strategy: Techniques for Analyzing Industries and Competitors, The Free Press, New York, NY., 1980.

[31] Power, R., "1999 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, Vol. 5, no. 1, 1999.

[32] President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," 1997.

[33] Quirke, B., Communicating Corporate Change: A Practical Guide to Communication and Corporate Strategy, McGraw-Hill, Maidenhead, Berkshire, England, 1996.

[34] Rezmierski, V., S. Deering, A. Fazio, and S. Ziobro, "Incident Cost Analysis and Modeling Report," The University of Michigan, 1998.

[35] Straub, D. W. and R. J. Welke, "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly,* Vol. 22, no. 4, 1998, pp. 441-469.

[36] System Security Study Committee, *Computers at Risk: Safe Computing in the Information Age,* National Research Council, 1991.

[37] Thierauf, R.J., *Effective Management and Evaluation of Information Technology*, Westport, Conn., Quorum Books, 1994.

[38] Vernon, R., "International Investment and International Trade in the Product Cycle," Quarterly Journal of Economics, Vol. 80, pp. 190-207.

[39] Weiss, J. and Wysocki, R., *5-Phase Project Management : A Practical Planning & Implementation Guide*, Perseus , 1992.

[40] Wood, C. C., "Writing InfoSec Policies," Computers and Security, Vol. 14, 1995.

[41] Wood, C. C., "Information Security Staffing Levels and the Standard of Due Care," *Computer Security Journal*, Vol. 13, 1997, pp. 1-8.

[42] Yourdon, E., *Modern Structured Analysis,* Englewood Cliffs, NJ, Yourdon Press, 1989.

Copyright © 1999 Andersen Consulting & CERIAS. All Rights Reserved.